The Hitchhiker's Guide to Online Anonymity

(Or "How I learned to start worrying and love privacy")

Version 0.9.9e (**draft**), July 2021 by AnonymousPlanet.

This guide is a DRAFT work in progress. While I am working constantly to correct issues, improve the content, general structure, and readability, it will probably never be "finished" and some parts might be incomplete as of this release.

Remember to check frequently for a new version of this guide.

Find it online at:

- Original: https://anonymousplanet.org [Archive.org] [Archive.today]
- Mirror: https://mirror.anonymousplanet.org [Archive.org] [Archive.today]
- Tor Mirror: http://thgtoa7imksbg7rit4grgijl2ef6kc7b56bp56pmtta4g354lydlzkqd.onion
- Archive.today over Tor: http://archivecaslytosk.onion/anonymousplanet.org/guide.html

PDF versions (best format for the best readability) of this guide at:

- Light Theme: https://anonymousplanet.org/guide.pdf [Mirror] [Archive org] [Tor Mirror]
- Dark Theme: https://anonymousplanet.org/guide-dark.pdf [Mirror] [Archive.org] [Tor Mirror]
- Both at CryptPad.fr https://cryptpad.fr/drive/#/2/drive/view/Ughm9CjQJCwB8BIppdtvj5zy4PyE-8Gxn11x9zaqJLI/

Feel free to submit issues using GitHub Issues at: https://github.com/AnonymousPlanet/thgtoa/issues
Feel free to come discuss ideas at:

- GitHub Discussions: https://github.com/AnonymousPlanet/thgtoa/discussions
- Matrix/Element: ```#online-anonymity:matrix.org``` https://matrix.to/#/#online-anonymity:matrix.org

Follow me on:

- Twitter at https://twitter.com/AnonyPla [Nitter] (cannot guarantee this account will stay up for long tho)
- Mastodon at https://mastodon.social/@anonypla.

Please consider donating if you enjoy the project and want to support the hosting fees (for the Tor hosting and the Tor Exit node).

There are several ways you could read this guide:

- You want to understand the current state of online privacy and anonymity not necessarily get too technical about it: Just read the Introduction, Requirements, Understanding some basics of how some information can lead back to you and how to mitigate those and A final editorial note sections.
- You want to do the above but also learn how to remove some online information about you: Just read the above and add the Removing some traces of your identities on search engines and various platforms.
- You want to do the above and create online anonymous identities online safely and securely: Read the whole guide.

Finally note that:

- This guide does mention and even recommends some commercial services in some sections (such as VPNs, CDNs, and hosting providers) but is not endorsed or sponsored by any of them in any way. There are no referral links and no commercial ties with any of these providers. This project is 100% non-profit.
- All external links to:

  - **Documents/Files** have an **[Archive.org]** link next to them for accessing content through Archive.org for increased privacy and in case the content goes missing. It is possible some links are not yet archived or outdated on archive.org in which case I encourage you to ask a new save if possible.
  - **YouTube Videos** have an **[Invidious]** link next to them for accessing content through an Invidious Instance (in this case yewtu.be hosted in the Netherlands) for increased privacy. See https://github.com/iv-org/invidious [Archive org] for more information.
  - **Twitter** have a **[Nitter]** link next to them for accessing content through a Nitter Instance (in this case nitter.fdn.fr hosted in France) for increased privacy. See https://github.com/zedeus/nitter [Archive.org] for more information.
  - **Wikipedia** have a **[Wikiless]** link next to them for accessing content through a Wikiless Instance (in this case Wikiless.org) for increased privacy. See https://codeberg.org/orenom/wikiless [Archive.org] for more information.
- **If you are reading this in PDF format, you will be seeing plenty of ``` in place of double quotes (""). These ``` should be ignored and are just there to facilitate conversion into Markdown/HTML format for on-line viewing.**

Contents:

Requirements:

- Be a permanent Adult resident in Germany where the courts have upheld up the legality of not using real names on online platforms (§13 VI of the German Telemedia Act of 2007[1,2]). **Alternatively, be an adult resident of any other country where you can validate and verify the legality of this guide yourself.**
- This guide will assume you already have access to some personal (Windows/Linux/MacOS) laptop computer (ideally not a work/shared device).
- Have patience as this process could take several weeks to finalize if you want to go through all the content.

[1] English translation of German Telemedia Act https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2016/02/Telemedia_Act__TMA_.pdf [Archive org]. Section 13, Article 6, "The service provider must enable the use of Telemedia and payment for them to occur anonymously or via a pseudonym where this is technically possible and reasonable. The recipient of the service is to be informed about this possibility. ".

[2] Wikipedia, Real-Name System Germany https://en.wikipedia.org/wiki/Real-name_system#Germany [Wikiless] [Archive.org]

- Have a little budget to dedicate to this process (you will need at least budget for an USB key).
- Have some free time on your hands to dedicate to this process (or a lot depending on the route you pick).
- Be prepared to read a lot of references (do read them), guides (do not skip them) and follow a lot of how-to tutorials thoroughly (do not skip them either).
- Don't be evil (for real this time)[3].

Introduction:

TLDR for the whole guide: "A strange game. The only winning move is not to play" [4].

Making a social media account with a pseudonym or artist/brand name is easy. And it is enough is most use cases to protect your identity as the next George Orwell. There are plenty of people using pseudonyms all over Facebook/Instagram/Twitter/LinkedIn/TikTok/Snapchat/Reddit/… But the vast majority of those are anything but anonymous and can easily be traced to their real identity by your local police officers, random people within the OSINT[5] (Open-Source Intelligence) community and trolls[6] on 4chan[7].

This is a good thing as most criminals/trolls are not really tech savvy and will be identified with ease. But this is also a bad thing as most political dissidents, human rights activists and whistleblowers can also be tracked rather easily.

This updated guide aims to provide introduction to various de-anonymization techniques, tracking techniques, id verification techniques and optional guidance to creating and maintaining **reasonably** anonymous identities online including social media accounts safely. This includes mainstream platforms and not only privacy friendly ones.

It is important to understand that the purpose of this guide is anonymity and not just privacy but many of the guidance you will find here will also help you improve your privacy and security even if you are not interested in anonymity. There is an important overlap in techniques and tools used for privacy, security, and anonymity but they differ at some point:

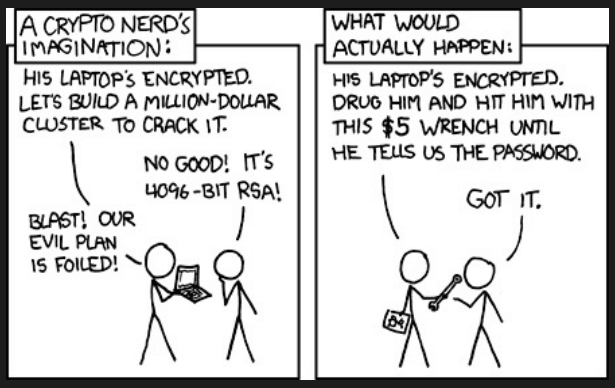
- **Privacy is about people knowing who you are but not knowing what you are doing.**
- **Anonymity is about people knowing what you are doing but not knowing who you are [8].**

[3] Wikipedia, Don't be evil https://en.wikipedia.org/wiki/Don%27t_be_evil [Wikiless] [Archive.org]
[4] YouTube, https://www.youtube.com/watch?v=6DGNZnfKYnU [Invidious]
[5] Wikipedia, OSINT https://en.wikipedia.org/wiki/Open-source_intelligence [Wikiless] [Archive.org]
[6] YouTube Internet Historian Playlist, HWNDU https://www.youtube.com/playlist?list=PLna1KTNJu3y09Tu70U6yPn28sekaNhOMY [Invidious]
[7] Wikipedia, 4chan https://en.wikipedia.org/wiki/4chan [Wikiless] [Archive.org]
[8] PIA, See this good article on the matter https://www.privateinternetaccess.com/blog/how-does-privacy-differ-from-anonymity-and-why-are-both-important/ [Archive.org] (disclaimer: this is not an endorsement or recommendation for this commercial service).

(Illustration from[9])

Will this guide help you protect yourself from the NSA, the FSB, Mark Zuckerberg, or the Mossad if they are out to find you? Probably not … Mossad will be doing "Mossad things" [10] and will probably find you no matter how hard you try to hide[11].

You must consider your threat model[12] before going further.



(Illustration by xkcd.com, licensed under CC BY-NC 2.5)

Will this guide help you protect your privacy from OSINT researchers like Bellingcat[13] , Doxing[14] trolls on 4chan[15] and others that have no access to the NSA toolbox? More likely. Tho I would not be so sure about 4chan.

Here is a basic simplified threat model for this guide:

This is the level where this guide will be able to help you. (realistically)

Threat (Adversaries)	• Unskilled • Unmotivated Your family, friends or boyfriend/ girlfriend are a bit curious about your activities.	• Unskilled • Motivated Advertisers are tracking you passively. HR people are just Googling you for a background check.	• Skilled • Unmotivated They could look into you but you're not doing anything of interest and you don't matter.	• Skilled • Motivated • Limited global resources Trolls, OSINT Researchers, Corporations, Local Law Enforcement….	• Highly Skilled • Highly Motivated • Unlimited global resources The NSA/FSB/MSS/ Mossad is looking for you.
Mitigations	• Set good passwords to protect your devices. • Use incognito modes. • Set your social accounts to private.	• Add 2FA to passwords. • Use Adblocking and incognito modes. • Set your accounts Private. • Use pseudonyms and branding.	• All of the previous and: • Use Tor Browser. • Use VPNs. • Consider using a dedicated phone number for accounts.	• This guide is your friend.	• Try magical amulets or invisibility cloaks. • Live in a submarine. • Fake your own death. They will find you over time.

[9] Medium.com, Privacy, Blockchain and Onion Routing https://medium.com/unitychain/privacy-blockchain-and-onion-routing-d5609c611841

[10] This World of Ours, James Mickens https://scholar.harvard.edu/files/mickens/files/thisworldofours.pdf [Archive org]

[11] XKCD, Security https://xkcd.com/538/ [Archive.org]

[12] Wikipedia, Threat Model https://en.wikipedia.org/wiki/Threat_model [Wikiless] [Archive.org]

[13] Bellingcat https://www.bellingcat.com/ [Archive.org]

[14] Wikipedia, Doxing https://en.wikipedia.org/wiki/Doxing [Wikiless] [Archive.org]

[15] YouTube, Internet Historian, The Bikelock Fugitive of Berkeley https://www.youtube.com/watch?v=muoR8Td44UE [Invidious]

(Note that the "magical amulets/submarine/fake your own death" jokes are quoted from [10])

Important Disclaimer: Jokes aside (magical amulet…). Of course, there are also advanced ways to mitigate attacks against such advanced and skilled adversaries but those are just out of scope of this guide. It is crucially important that you understand the limits of the threat model of this guide. And therefore, this guide will not double in size to help with those advanced mitigations as this is just too complex and will require a very high knowledge that is not expected from the targeted audience of this guide.

The EFF provides a few security scenarios of what you should consider depending on your activity. While some of those tips might not be within the scope of this guide (more about Privacy than Anonymity), they are still worth reading as examples. See https://ssd.eff.org/en/module-categories/security-scenarios [Archive.org].

There are also quite a few more serious ways of making your threat model such as:

- LINDDUN https://www.linddun.org/ [Archive org]
- STRIDE https://en.wikipedia.org/wiki/STRIDE_%28security%29 [Wikiless] [Archive.org]
- DREAD https://en.wikipedia.org/wiki/DREAD_%28risk_assessment_model%29 [Wikiless] [Archive org]
- PASTA https://versprite.com/tag/pasta-threat-modeling/ [Archive.org]

And there are quite a few others too, see:

- https://insights.sei.cmu.edu/blog/threat-modeling-12-available-methods/ [Archive.org]
- https://www.geeksforgeeks.org/threat-modelling/ [Archive.org]

You can find some introduction on these on these projects:

- OWASP https://cheatsheetseries.owasp.org/cheatsheets/Threat_Modeling_Cheat_Sheet.html [Archive.org]
- Online Operations Security https://github.com/devbret/online-opsec/ [Archive.org]

It is also very important **again** to understand this guide is the humble result of years of experience, learning and testing **from a single individual** (myself) and that many of those systems that aim to prevent anonymity are opaque proprietary closed-source systems. Many of those guidelines are based on experience, on referenced studies and recommendations by other people and projects. These experiences take a lot of time, resources and are sometimes far from being scientific. **There might be some wrong or outdated information in this guide too because I am not omniscient and humans make mistakes (feel free to report any using GitHub Issues). Your mileage may vary (a lot). Use at your own risk. Please do not take this guide as a definitive truth for everything because it is not. Plenty of mistakes have been written in the guide during the many previous drafts and fixed later when I was made aware of them. I have no doubts there are still some mistakes in here right now. All of those are fixed as soon as possible when discovered.**

You might think this guide has no legitimate use but there are many[16, 17, 18, 19, 20, 21, 22] such as:

- Evading Online Censorship
- Evading Online Oppression
- Evading Online Stalking, Doxxing, and Harassment
- Evading Online Unlawful Government Surveillance
- Anonymous Online Whistle Blowing
- Anonymous Online Activism

---

[16] BBC News, Tor Mirror https://www.bbc.com/news/technology-50150981 [Archive.org]

[17] GitHub, Real World Onion websites https://github.com/alecmuffett/real-world-onion-sites [Archive.org]

[18] Tor Project, Who Uses Tor https://2019.www.torproject.org/about/torusers.html.en [Archive.org]

[19] Whonix Documentation, The importance of Anonymity https://www.whonix.org/wiki/Anonymity [Archive.org]

[20] Geek Feminism, https://geekfeminism.wikia.org/wiki/Who_is_harmed_by_a_%22Real_Names%22_policy%3F [Archive.org]

[21] Tor Project, Tor Users https://2019.www.torproject.org/about/torusers.html.en [Archive.org]

[22] PrivacyHub, Internet Privacy in the Age of Surveillance https://www.cyberghostvpn.com/privacyhub/internet-privacy-surveillance/ [Archive.org]

- Anonymous Online Journalism
- Anonymous Online Legal Practice
- Anonymous Online Academic Activities (For instance accessing scientific research where such resources are blocked). See note below.
- …

Note: that if you are having trouble accessing any of the many academic articles referenced in this guide, feel free to use Sci-Hub (https://en.wikipedia.org/wiki/Sci-Hub [Wikiless] [Archive.org]) or LibGen (https://en.wikipedia.org/wiki/Library_Genesis [Wikiless] [Archive.org]) for finding and reading them. Because science should be free. All of it.

This guide is written with hope for those **good intended individuals** who might not be knowledgeable enough to consider the big picture of online anonymity and privacy.

This guide is not intended for:

- Creating machine accounts of any kind (bots).
- Creating impersonation accounts of existing people (such as identity theft).
- Helping malicious actors conduct unlawful or unethical activities (such as trolling, stalking, disinformation, misinformation, harassment, or any criminal activity).
- Use by minors.

Feel free to report issues, recommend improvements or start a discussion on the GitHub repository if you want.

Again, use at your own risk. Anything in here is not legal advice and you should verify compliance with your local law before use (IANAL[23]). "Trust but verify"[24] all the information yourself (or even better, "Never Trust, always verify"[348]). I strongly encourage you to inform yourself and do not hesitate to check any information in this guide with outside sources in case of doubt. Please do report any mistake you spot to me as I welcome criticism. Even harsh criticism and usually make the necessary corrections as quickly as possible.

Understanding some basics of how some information can lead back to you and how to mitigate some:

There are many ways you can be tracked besides browser cookies and ads, your e-mail, and your phone number. And if you think only the Mossad or the NSA/FSB can find you, you would be terribly wrong.

You might consider viewing this good YouTube playlist as an introduction before going further: https://www.youtube.com/playlist?list=PL3KeV6Ui_4CayDGHw64OFXEPHgXLkrtJO [Invidious] (from the Go Incognito project https://github.com/techlore-official/go-incognito [Archive.org]). This guide will cover many of those topics with more details and references as well as some additional topics not covered within that series but I would recommend the series as an introduction and it will just take you 2 or 3 hours to watch it all.

Now, here is a non-exhaustive list of some of the many ways you could be tracked and de-anonymized:

Your Network:

Your IP address:

Disclaimer: this whole paragraph is about your public facing Internet IP and not your local network IP

Your IP address[25] is the most known and obvious way you can be tracked. That IP is the IP you are using at the source. This is where you connect to the internet. That IP is usually provided by your ISP (Internet Service Provider) (xDSL, Mobile, Cable, Fiber, Cafe, Bar, Friend, Neighbor). Most countries have data retention regulations[26] which

[23] Wikipedia, IANAL https://en.wikipedia.org/wiki/IANAL [Wikiless] [Archive org]

[24] Wikipedia, Trust but verify https://en.wikipedia.org/wiki/Trust,_but_verify [Wikiless] [Archive.org]

[25] Wikipedia, IP Address, https://en.wikipedia.org/wiki/IP_address [Wikiless] [Archive.org]

[26] Wikipedia; Data Retention https://en.wikipedia.org/wiki/Data_retention [Wikiless] [Archive.org]

mandates keeping logs of who is using what IP at a certain time/date for up to several years or indefinitely. Your ISP can tell a third party that you were using a specific IP at a specific date and time, years after the fact. If that IP (the origin one) leaks at any point for any reason, it can be used to track down you directly. In many countries, you will not be able to have internet access without providing some form of identification to the provider (address, ID, real name, e-mail …).
Useless to say that most platforms (such as social networks) will also keep (sometimes indefinitely) the IP addresses you used to sign-up and sign-in to their services.

Here are some online resources you can use to find some information about your current **public IP** right now:

- Find your IP:
  - https://resolve.rs/
  - https://www.dnsleaktest.com/ (Bonus, check your IP for DNS leaks)
- Find your IP location or the location of any IP:
  - https://resolve.rs/ip/geolocation.html
- Find if an IP is "suspicious" or has downloaded "things" on some public resources:
  - https://www.virustotal.com/gui/home/search
  - https://iknowwhatyoudownload.com
- Registration information of an IP (most likely your ISP or the ISP of your connection who most likely know who is using that IP at any time):
  - https://whois.domaintools.com/
- Check for open-services or open-devices on an IP (especially if there are leaky Smart Devices on it):
  - https://www.shodan.io/host/185.220.101.134 (replace the IP by your IP or any other, or change in the search box, this example IP is a Tor Exit node)
- Various tools to check your IP such as blacklists checkers and more:
  - https://www.whatismyip.com
  - https://browserleaks.com/
- Would you like to know if you are connected through Tor?
  - https://check.torproject.org

For those reasons, we will need to obfuscate that origin IP (the one tied to your identification) or hide it as much as we can through a combination of various means:

- Using a public Wi-Fi service (free).
- Using the Tor Anonymity Network[27] (free).
- Using VPN[28] services anonymously (anonymously paid with cash or Monero).

All those will be explained later in this guide.

Your DNS and IP requests:

DNS stands for "Domain Name System"[29] and is a service used by your browser (and other apps) to find the IP addresses of a service. It is pretty much a huge "contact list" (phone book for older people) that works like asking it a name and it returns the number to call. Except it returns an IP instead.

Every time your browser wants to access a certain service such as Google through www.google.com. Your Browser (Chrome or Firefox) will query a DNS service to find the IP addresses of the Google web servers.

Here is a video explaining DNS visually if you are already lost: https://www.youtube.com/watch?v=vrxwXXytEuI [Invidious]

Usually, the DNS service is provided by your ISP and automatically configured by the network you are connecting to. This DNS service could also be subject to data retention regulations or will just keep logs for other reasons (data

[27] Wikipedia, Tor Anonymity Network https://en.wikipedia.org/wiki/Tor_(anonymity_network) [Wikiless] [Archive org]
[28] Wikipedia, VPN https://en.wikipedia.org/wiki/Virtual_private_network [Wikiless] [Archive.org]
[29] Wikipedia, DNS https://en.wikipedia.org/wiki/Domain_Name_System [Wikiless] [Archive.org]

collection for advertising purposes for instance). Therefore, this ISP will be capable of telling everything you did online just by looking at those logs which can in turn be provided to an adversary. Conveniently this also the easiest way for many adversaries to apply censoring or parental control by using DNS blocking[30]. The provided DNS servers will give you a different address (than their real one) for some websites (like redirecting thepiratebay to some government website). Such blocking is widely applied worldwide for certain sites[31].

Using a private DNS service or your own DNS service would mitigate these issues but the other problem is that most of those DNS requests are by default still sent in clear text (unencrypted) over the network. Even if you browse PornHub in an incognito Window, using HTTPS and using a private DNS service, chances are very high that your browser will send a clear text unencrypted DNS request to some DNS servers asking basically "So what's the IP address of www.pornhub.com?".

Because it is not encrypted, your ISP and/or any other adversary could still intercept (using a Man-in-the-middle attack[88]) your request will know and possibly log what your IP was looking for. The same ISP can also tamper with the DNS responses even if you are using a private DNS. Rendering the use of a private DNS service useless.

As a bonus, many devices and apps will use hardcoded DNS servers bypassing any system setting you could set. This is for example the case with most (70%) Smart TVs and a large part (46%) of Game Consoles[32]. For these devices, you will have to force them[33] to stop using their hardcoded DNS service which could make them stop working properly.

A solution to this is to use encrypted DNS using DoH (DNS over HTTPS[34]), DoT (DNS over TLS[35]) with a private DNS server (this can be self-hosted locally with a solution like pi-hole[36], remotely hosted with a solution like nextdns.io or using the solutions provider by your VPN provider or the Tor network). This should prevent your ISP or some middle-man from snooping on your requests … except it might not.

Small in-between disclaimer: **This guide does not necessarily endorse or recommends Cloudflare services even if it is mentioned several times in this section for technical understanding.**

Unfortunately, the TLS protocol used in most HTTPS connections in most Browsers (Chrome/Brave/Ungoogled-Chromium among them) will leak the Domain Name again through SNI[37] handshakes (this can be checked here at Cloudflare: https://www.cloudflare.com/ssl/encrypted-sni/ [Archive.org]). **As of the writing of this guide, only Firefox based browsers supports ECH (Encrypted Client Hello[38] previously known as eSNI[39]) on some websites which will encrypt everything end to end (in addition to using a secure private DNS over TLS/HTTPS) and will allow you to hide your DNS requests from a third party[40].** And this option is not enabled by default either so you will have to enable it yourself.

---

[30] Wikipedia, DNS Blocking https://en.wikipedia.org/wiki/DNS_blocking [Wikiless] [Archive org]

[31] CensoredPlanet https://censoredplanet.org/ [Archive org]

[32] ArXiv, Characterizing Smart Home IoT Traffic in the Wild https://arxiv.org/pdf/2001.08288.pdf [Archive.org]

[33] Labzilla.io, Your Smart TV is probably ignoring your Pi-Hole https://labzilla.io/blog/force-dns-pihole [Archive.org]

[34] Wikipedia, DNS over HTTPS: https://en.wikipedia.org/wiki/DNS_over_HTTPS [Wikiless] [Archive org]

[35] Wikipedia, DNS over TLS, https://en.wikipedia.org/wiki/DNS_over_TLS [Wikiless] [Archive.org]

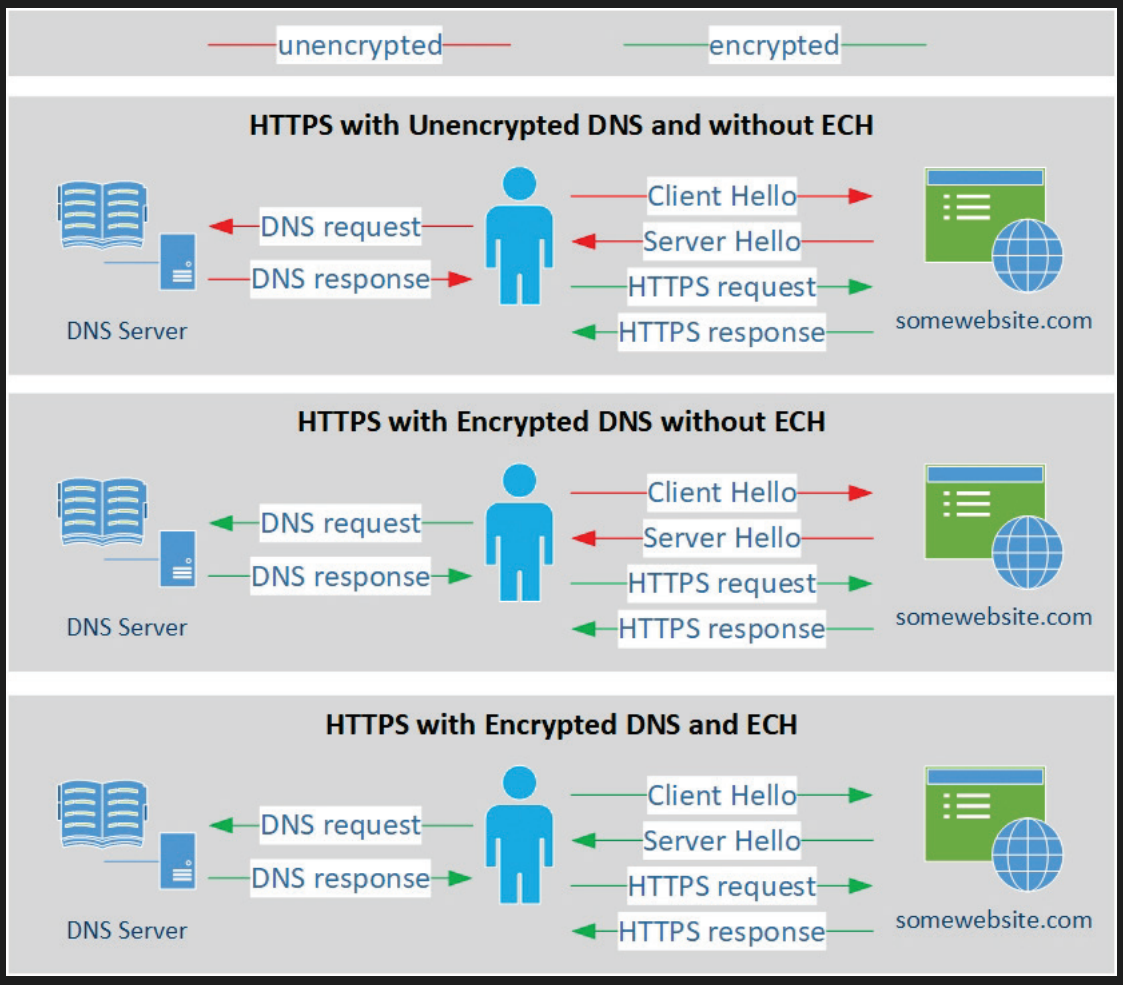
[36] Wikipedia, Pi-Hole https://en.wikipedia.org/wiki/Pi-hole [Wikiless] [Archive org]

[37] Wikipedia, SNI https://en.wikipedia.org/wiki/Server_Name_Indication [Wikiless] [Archive.org]

[38] Wikipedia, ECH, https://en.wikipedia.org/wiki/Server_Name_Indication#Encrypted_Client_Hello [Wikiless] [Archive.org]

[39] Wikipedia, eSNI https://en.wikipedia.org/wiki/Server_Name_Indication#Encrypted_Client_Hello [Wikiless] [Archive.org]

[40] Usenix.org, On the Importance of Encrypted-SNI (ESNI) to Censorship Circumvention https://www.usenix.org/system/files/foci19-paper_chai_0.pdf [Archive org]



In addition to limited browser support, only Web Services and CDNs[41] behind Cloudflare CDN support ECH/eSNI at this stage[42]. This means that ECH and eSNI are not supported (as of the writing of this guide) by most mainstream platforms such as:

- Amazon (including AWS, Twitch…)
- Microsoft (including Azure, OneDrive, Outlook, Office 365…)
- Google (including Gmail, Google Cloud…)
- Apple (including iCloud, iMessage…)
- Reddit
- YouTube
- Facebook
- Instagram
- Twitter
- GitHub
- …

Some countries like Russia[43] and China[44] will block ECH/eSNI handshakes at network level to allow snooping and prevent bypassing censorship. Meaning you will not be able to establish an HTTPS connection with a service if you do not allow them to see what it was.

[41] Wikipedia, CDN https://en.wikipedia.org/wiki/Content_delivery_network [Wikiless] [Archive.org]

[42] Cloudflare, Good-bye ESNI, hello ECH! https://blog.cloudflare.com/encrypted-client-hello/ [Archive.org]

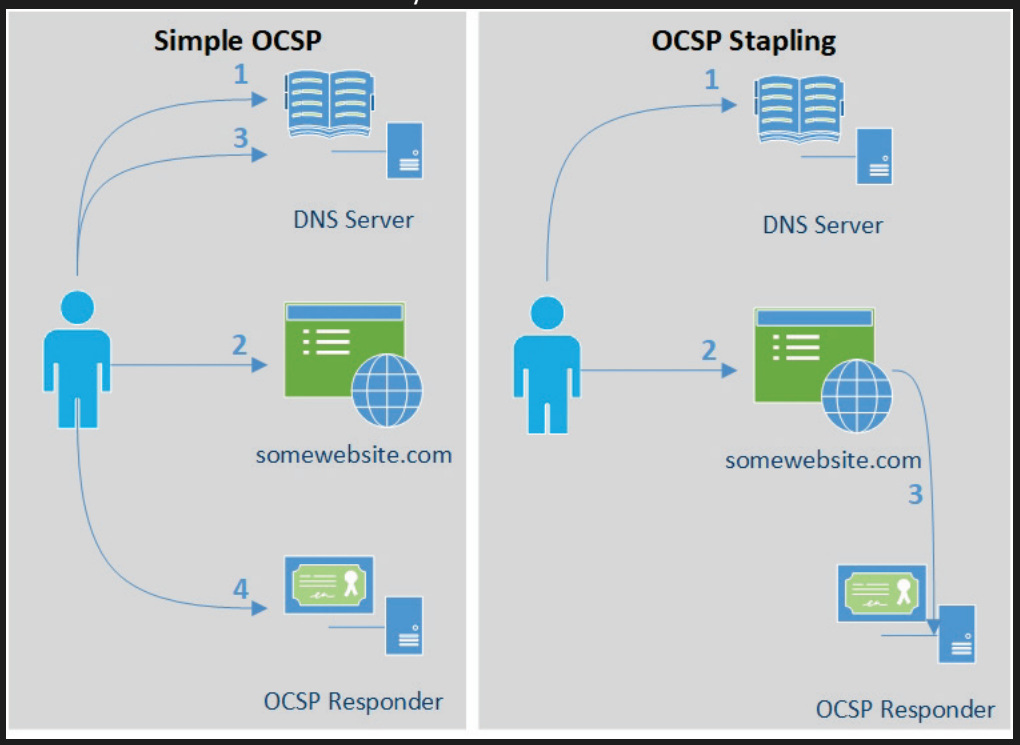
[43] ZDNET, Russia wants to ban the use of secure protocols such as TLS 1.3, DoH, DoT, ESNI https://www.zdnet.com/article/russia-wants-to-ban-the-use-of-secure-protocols-such-as-tls-1-3-doh-dot-esni/ [Archive org]

[44] ZDNET, China is now blocking all encrypted HTTPS traffic that uses TLS 1.3 and ESNI https://www.zdnet.com/article/china-is-now-blocking-all-encrypted-https-traffic-using-tls-1-3-and-esni/ [Archive.org]

The issues do not end here. Part of the HTTPS TLS validation is called OCSP[45] and this protocol used by Firefox based browsers will leak metadata in the form of the serial number of the certificate of the website you are visiting. An adversary can then easily find which website you are visiting by matching the certificate number[46]. This issue can be mitigated by using OCSP stapling[47]. Unfortunately, this is enabled but not enforced by default in Firefox/Tor Browser. But the website you are visiting must also be supporting it and not all do. Chromium based browser on the other hand use a different system called CRLSets[48,49] which is arguably better.

Here is a list of how various browser behave in relation with OCSP: https://www.ssl.com/blogs/how-do-browsers-handle-revoked-ssl-tls-certificates/ [Archive.org]

Here is an illustration of the issue you could encounter on Firefox based browsers:



Finally, even if you use a custom encrypted DNS server (DoH or DoT) with ECH/eSNI support and OCSP stapling, it might still not be enough as traffic analysis studies[50] have shown it is still possible to reliably fingerprint and block unwanted requests. Only DNS over Tor was able to demonstrate efficient DNS Privacy in recent studies but even that can still be defeated by other means (see Your Anonymized Tor/VPN traffic).

One could also decide to use a Tor Hidden DNS Service or ODoH (Oblivious DNS over HTTPS[51]) to further increase privacy/anonymity but **unfortunately**, as far as I know, these methods are only provided by Cloudflare as of this writing (https://blog.cloudflare.com/welcome-hidden-resolver/ [Archive.org], https://blog.cloudflare.com/oblivious-dns/ [Archive org]). I **personally** think these are viable and reasonably secure technical options but there is also a moral choice if you want to use Cloudflare or not (despite the risk posed by some researchers[52]).

---

[45] Wikipedia, OCSP https://en.wikipedia.org/wiki/Online_Certificate_Status_Protocol [Wikiless] [Archive.org]

[46] Madaidans Insecurities, Why encrypted DNS is ineffective https://madaidans-insecurities.github.io/encrypted-dns.html [Archive org]

[47] Wikipedia, OCSP Stapling https://en.wikipedia.org/wiki/OCSP_stapling [Wikiless] [Archive.org]

[48] Chromium Documentation, CRLSets https://dev.chromium.org/Home/chromium-security/crlsets [Archive org]

[49] ZDNet, Chrome does certificate revocation better https://www.zdnet.com/article/chrome-does-certificate-revocation-better/ [Archive org]

[50] KUL, Encrypted DNS==⇒Privacy? A Traffic Analysis Perspective https://www.esat.kuleuven.be/cosic/publications/article-3153.pdf [Archive.org]

[51] ResearhGate, Oblivious DNS: Practical Privacy for DNS Queries https://www.researchgate.net/publication/332893422_Oblivious_DNS_Practical_Privacy_for_DNS_Queries [Archive.org]

[52] Nymity.ch, The Effect of DNS on Tor's Anonymity https://nymity.ch/tor-dns/ [Archive.org]

Lastly, there is also this new option called DoHoT which stands for DNS over HTTPS over Tor which could also further increase your privacy/anonymity and which you could consider if you are more skilled with Linux. See https://github.com/alecmuffett/dohot [Archive.org]. This guide will not help you with this one at this stage but it might be coming soon.

Here is an illustration showing the current state of DNS and HTTPS privacy based on my current knowledge.

As for your normal daily use (non-sensitive), remember that only Firefox based browsers support ECH (formerly eSNI) so far and that it is only useful with websites hosted behind Cloudflare CDN at this stage. If you prefer a Chrome based version (which is understandable for some due to some better integrated features like on-the-fly

Translation), then I would recommend the use of Brave instead which supports all Chrome extensions and offers much better privacy than Chrome. Alternatively, if you do not trust Brave, you could also use Ungoogled-Chromium (https://github.com/Eloston/ungoogled-chromium [Archive.org]).

But the story does not stop there right. Now because after all this, even if you encrypt your DNS and use all possible mitigations. Simple IP requests to any server will probably allow an adversary to still detect which site you are visiting. And this is simply because the majority of websites have unique IPs tied to them as explained here: https://blog.apnic.net/2019/08/23/what-can-you-learn-from-an-ip-address/ [Archive.org]. This mean that an adversary can create a dataset of known websites for instance including their IPs and then match this dataset against the IP you request. In most cases, this will result in a correct guess of the website you are visiting. This means that despite OCSP stapling, despite ECH/eSNI, despite using Encrypted DNS … An adversary can still guess the website you are visiting anyway.

Therefore, to mitigate all these issues (as much as possible and as best as we can), this guide will later recommend two solutions: Using Tor and a virtualized (See Appendix W: Virtualization) multi-layered solution of VPN over Tor solution. Other options will also be explained (Tor over VPN, VPN only, No Tor/VPN) but are less recommended.

Your RFID enabled devices:

RFID stands for Radio-frequency identification[53], it is the technology used for instance for contactless payments and various identification systems. Of course, your smartphone is among those devices and has RFID contactless payment capabilities through NFC[54]. As with everything else, such capabilities can be used for tracking by various actors.

But unfortunately, this is not limited your smartphone and you also probably carry some amount of RFID enabled device with you all the time such as:

- Your contactless enabled credit/debit cards
- Your store loyalty cards
- Your transportation payment cards
- Your work-related access cards
- Your car keys
- Your national ID or driver license
- Your passport
- The price/anti-theft tags on object/clothing
- …

While all these cannot be used to de-anonymize you from a remote online adversary, they can be used to narrow down a search if your approximate location at a certain time is known. For instance, you cannot rule out that some stores will effectively scan (and log) all RFID chips passing through the door. They might be looking for their loyalty cards but are also logging others along the way. Such RFID tags could be traced to your identity and allow for de-anonymization.

More information over at Wikipedia: https://en.wikipedia.org/wiki/Radio-frequency_identification#Security_concerns [Wikiless] [Archive.org] and https://en.wikipedia.org/wiki/Radio-frequency_identification#Privacy [Wikiless] [Archive.org]

The only way to mitigate this problem is to have no RFID tags on you or to shield them again using a type of faraday cage. You could also use specialized wallets/pouches that specifically block RFID communications. Many of those are now made by well-known brands such as Samsonite[55].

---

[53] Wikipedia, RFID https://en.wikipedia.org/wiki/Radio-frequency_identification [Wikiless] [Archive org]

[54] Wikipedia, NFC https://en.wikipedia.org/wiki/Near-field_communication [Wikiless] [Archive.org]

[55] Samsonite Online Shop, RFID accessories, https://shop.samsonite.com/accessories/rfid-accessories/ [Archive.org]

See Appendix N: Warning about smartphones and smart devices

The Wi-Fis and Bluetooth devices around you:

Geolocation is not only done by using mobile antennas triangulation. It is also done using the Wi-Fis and Bluetooth devices around you. Operating systems makers like Google (Android[56]) and Apple (IOS[57]) maintain a convenient database of most Wi-Fi access points, Bluetooth devices and their location. When your Android smartphone or iPhone is on (and not in Plane mode), it will scan passively (unless you specifically disable this feature in the settings) Wi-Fi access points and Bluetooth devices around you and will be able to geolocate you with more precision than when using a GPS.

This allows them to provide accurate locations even when GPS is off but it also allows them to keep a convenient record of all Bluetooth devices all over the world. Which can then be accessed by them or third parties for tracking.

Note: If you have an Android smartphone, Google probably knows where it is no matter what you do. You cannot really trust the settings. The whole operating system is built by a company that wants your data. Remember that if it is free then you are the product.

But that is not what all those Wi-Fis access points can do. Recently developed techs could even allow someone to track your movements accurately just based on radio interferences. What this means is that it is possible to track your movement inside a room/building based on the radio signals passing through. This might seem like a tinfoil hat conspiracy theory claim but here are the references[58] with demonstrations showing this tech in action: http://rfpose.csail.mit.edu/ [Archive.org] and the video here: https://www.youtube.com/watch?v=HgDdaMy8KNE [Invidious]

You could therefore imagine many uses cases for such technologies like recording who enters specific buildings/offices (hotels, hospitals, or embassies for instance) and then discover who meets who and where by tracking them from outside. Even if they have no smartphone on them.

Again, such issue could only be mitigated by being in room/building that would act as a faraday cage.

Here is another video of the same kind of tech in action: https://www.youtube.com/watch?v=FDZ39h-kCS8 [Invidious]

See Appendix N: Warning about smartphones and smart devices

---

[56] Google Android Help, Android Location Services https://support.google.com/accounts/answer/3467281?hl=en [Archive.org]

[57] Apple Support, Location Services and Privacy https://support.apple.com/en-us/HT207056 [Archive.org]

[58] State University of New York, Towards 3D Human Pose Construction Using Wi-Fi https://cse.buffalo.edu/~lusu/papers/MobiCom2020.pdf [Archive.org]

Malicious/Rogue Wi-Fi Access Points:

These have been used since at least since 2008 using an attack called "Jasager"[59] and can be done by anyone using self-built tools or using commercially available devices such as Wi-Fi Pineapple[60].

Here are some videos explaining more about the topic:

- HOPE 2020, https://archive.org/details/hopeconf2020/20200725_1800_Advanced_Wi-Fi_Hacking_With_%245_Microcontrollers.mp4
- YouTube, Hak5, Wi-Fi Pineapple Mark VII https://www.youtube.com/watch?v=7v3JR4Wlw4Q [Invidious]

These devices can fit in a small bag and can take over the Wi-Fi environment of any place within their range. For instance, a Bar/Restaurant/Café/Hotel Lobby. These devices can force Wi-Fi clients to disconnect from their current Wi-Fi (using de-authentication, disassociation attacks[61]) while spoofing the normal Wi-Fi networks at the same location. They will continue to perform this attack until your computer or yourself decides to try to connect to the rogue AP.

These devices can then mimic a captive portal[62] with the exact same layout as the Wi-Fi you are trying to access (for instance an Airport Wi-Fi registration portal). Or they could just give you open access internet that they will themselves get from the same place.

Once you are connected through the Rogue AP, this AP will be able to execute various man-in-the-middle attacks to perform analysis on your traffic. These could be malicious redirections or just simple traffic sniffing. These can then easily identify any client that would for instance try to connect to a VPN server or to the Tor Network.

This can be useful when you know someone you want to de-anonymize is in a crowded place but you do not know who. This would allow such an adversary to possibly fingerprint any website you visit despite the use of HTTPS, DoT, DoH, ODoH, VPN or Tor using traffic analysis as pointed above in the DNS section.

These can also be used to carefully craft and serve you advanced phishing webpages that would harvest your credentials or try to make you install a malicious certificate allowing them to see your encrypted traffic.

Your Anonymized Tor/VPN traffic:

Tor and VPNs are not silver bullets. Many advanced techniques have been developed and studied to de-anonymize encrypted Tor traffic over the years[63]. Most of those techniques are Correlation attacks that will correlate your network traffic in one way or another to logs or datasets. Here are some classic examples:

- Correlation Fingerprinting Attack: As illustrated (simplified) below, this attack will fingerprint[64] your encrypted traffic (like the websites you visited) just based on the analysis of your encrypted traffic (without decrypting it). It can do so with a whopping 96% success rate. Such fingerprinting can be used by an adversary that has access to your source network to figure out some of your encrypted activity (such as which websites you visited).

[59] Digi.Ninja, Jasager https://digi.ninja/jasager/ [Archive.org]

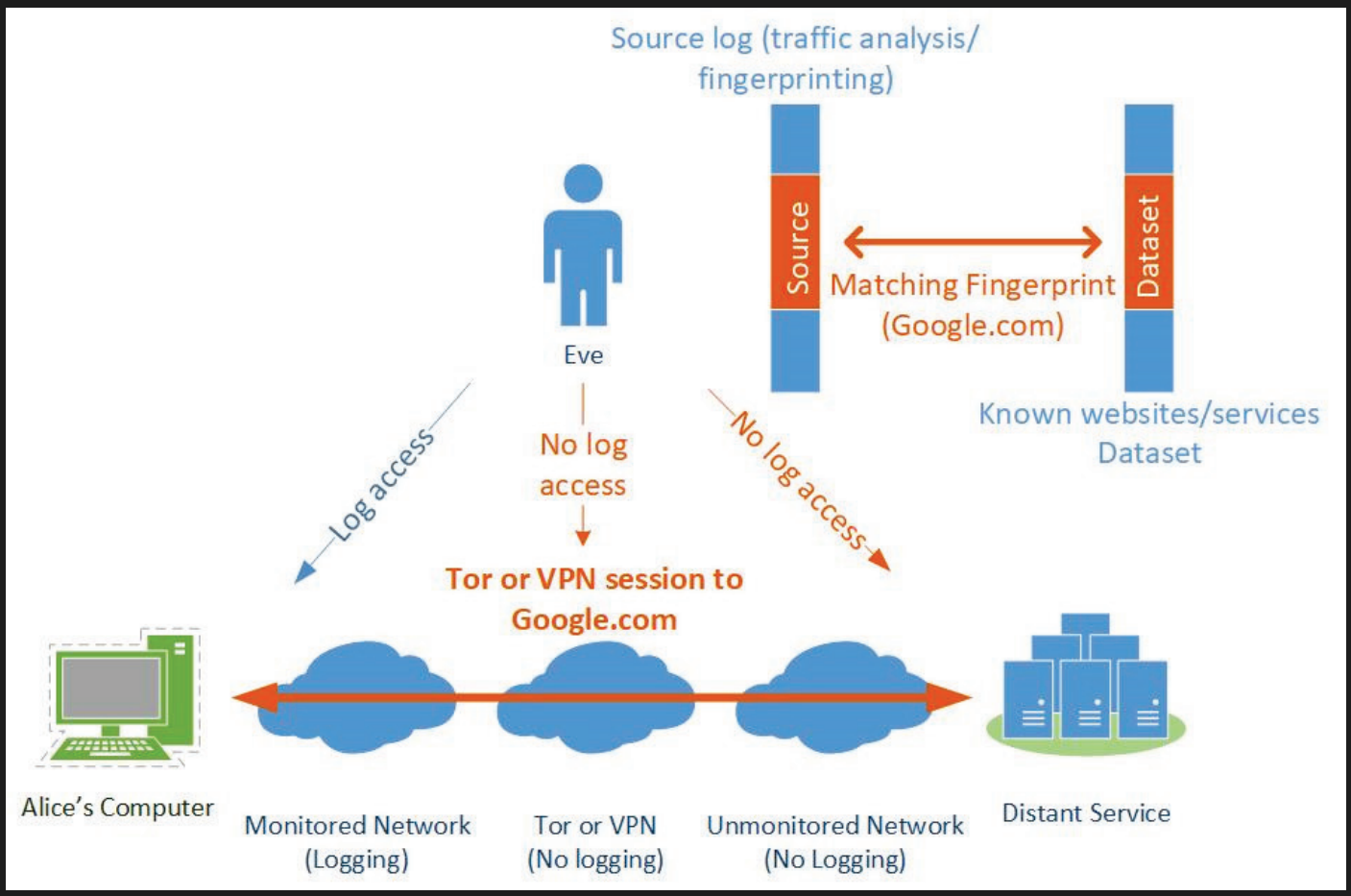
[60] Hak5 Shop, Wi-Fi Pineapple https://shop.hak5.org/products/wifi-pineapple [Archive.org]

[61] Wikipedia, Deautentication Attack https://en.wikipedia.org/wiki/Wi-Fi_deauthentication_attack [Wikiless] [Archive.org]

[62] Wikipedia, Capture Portal https://en.wikipedia.org/wiki/Captive_portal [Wikiless] [Archive.org]

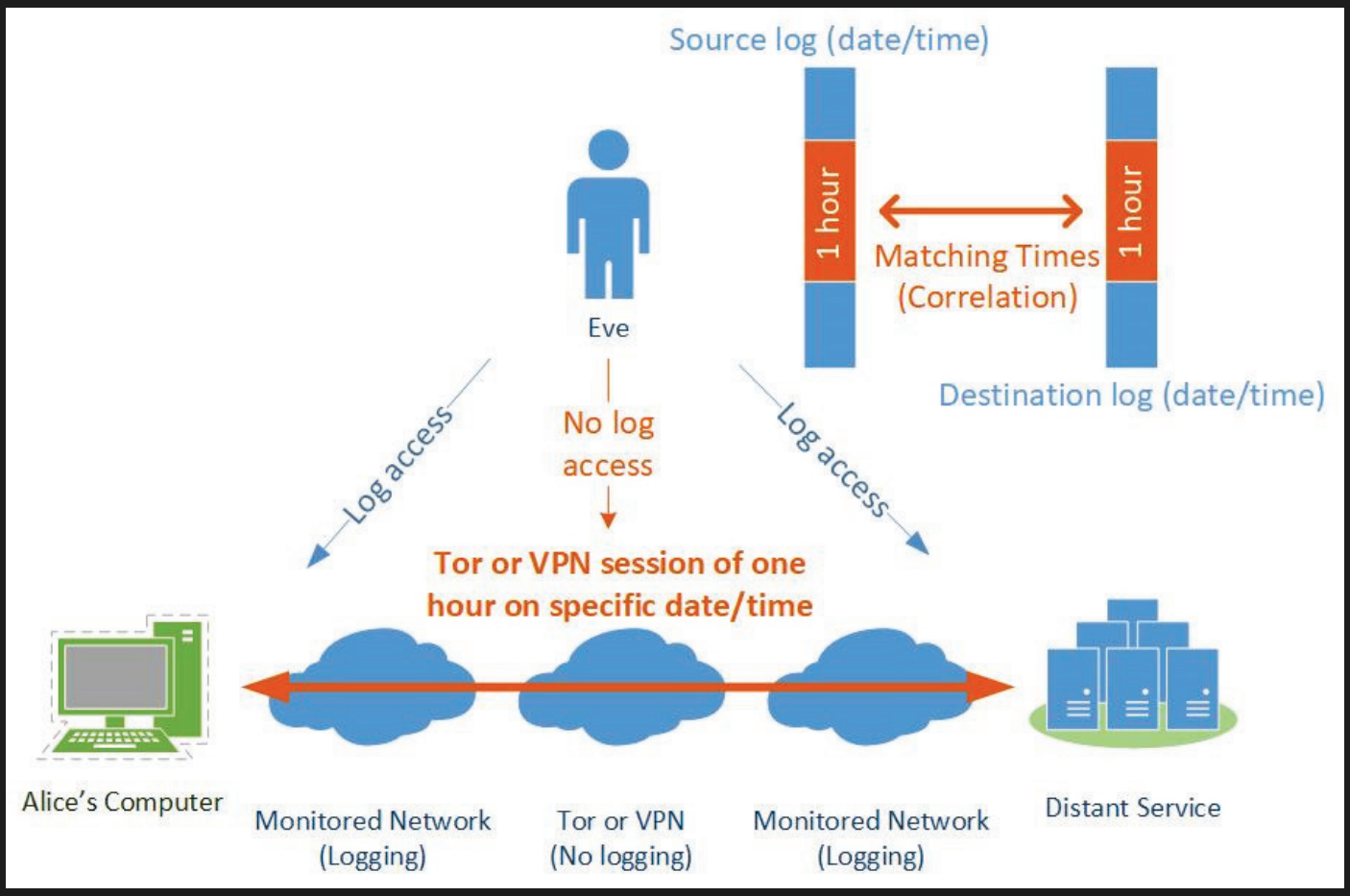
[63] HackerFactor Blog, Deanonymizing Tor Circuits https://www.hackerfactor.com/blog/index.php?/archives/868-Deanonymizing-Tor-Circuits.html [Archive.org]

[64] KU Leuven, Website Fingerprinting through Deep Learning https://distrinet.cs.kuleuven.be/software/tor-wf-dl/ [Archive org]

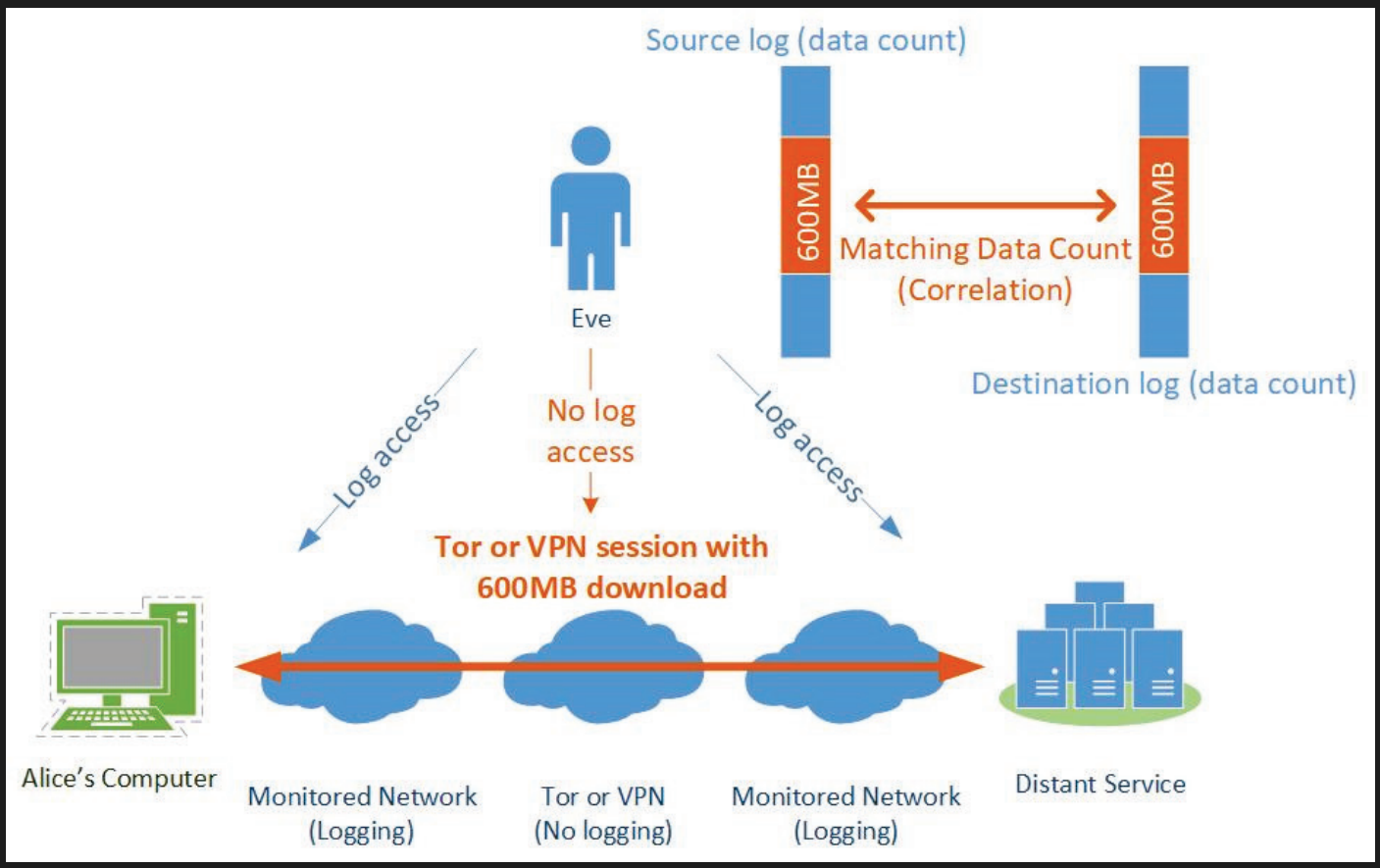


- Correlation Timing Attacks: As illustrated (simplified) below, an adversary that has access to network connection logs (IP or DNS for instance, remember that most VPN servers and most Tor nodes are known and publicly listed) at the source and at the destination could correlate the timings to de-anonymize you without requiring any access to the Tor or VPN network in between. A real use case of this technique was done by the FBI in 2013 to de-anonymize[65] a bomb threat hoax at Harvard University.

[65] DailyDot, How Tor helped catch the Harvard bomb threat suspect https://www.dailydot.com/unclick/tor-harvard-bomb-suspect/ [Archive org]



- Correlation Counting Attacks: As illustrated (simplified) below, an adversary that has no access to detailed connection logs (cannot see that you used Tor or Netflix) but has access to data counting logs could see that you have downloaded 600MB on a specific time/date that matches the 600MB upload at the destination. This correlation can then be used to de-anonymize you over time.



There are ways to mitigate these such as:

- Do not use Tor/VPNs to access services that are on the same network (ISP) as the destination service. For example, do not connect to Tor from your University Network to access a University Service anonymously. Instead use a different source point (such as a public Wi-Fi) that cannot be correlated easily by an adversary.
- Do not use Tor/VPN from an obviously monitored network (such as a corporate/governmental Network) but instead try to find an unmonitored network such as a public Wi-Fi or a residential Wi-Fi.
- Use multiple layers (such as what will be recommended in this guide later: VPN over Tor) so that an adversary might be able to see that someone connected to the service through Tor but will not be able to see that it was you because you were connected to a VPN and not the Tor Network.

Be aware again that this might not be enough against a motivated global adversary[66] with wide access to global mass surveillance. Such adversary might have access to logs no matter where you are and could use those to de-anonymize you.

Be also aware that all the other methods described in this guide such as Behavioral analysis can also be used to deanonymize Tor users indirectly (see further Your Digital Fingerprint, Footprint, and Online Behavior).

I also strongly recommend reading this very good, complete and thorough guide on many Attack Vectors on Tor: https://github.com/Attacks-on-Tor/Attacks-on-Tor [Archive.org] as well as this recent research publication https://www.researchgate.net/publication/323627387_Shedding_Light_on_the_Dark_Corners_of_the_Internet_A_Survey_of_Tor_Research [Archive.org]

As well as this great series of blog posts: https://www.hackerfactor.com/blog/index.php?/archives/906-Tor-0day-The-Management-Vulnerability.html [Archive.org]

(In their defense, it should also be noted that Tor is not designed to protect against a Global adversary. For more information see https://svn-archive.torproject.org/svn/projects/design-paper/tor-design.pdf [Archive.org] and specifically, "Part 3. Design goals and assumptions.".)

Lastly, do remember that using Tor can already be considered a suspicious activity[67] and its use could be considered malicious by some[68].

This guide will later propose some mitigations to such attacks by changing your origin from the start (using public wi-fi's for instance).

Some Devices can be tracked even when offline:

You have seen this in action/spy/Sci-Fi movies and shows, the protagonists always remove the battery of their phones to make sure it cannot be used. Most people would think that's overkill. Well, unfortunately no, this is now becoming true at least for some devices:

- iPhones and iPads (IOS 13 and above)[69, 70]
- Samsung Phones (Android 10 and above)[71]
- MacBooks (MacOS 10.15 and above)[72]

---

[66] ArsTechnica, How the NSA can break trillions of encrypted Web and VPN connections https://arstechnica.com/information-technology/2015/10/how-the-nsa-can-break-trillions-of-encrypted-web-and-vpn-connections/ [Archive.org]

[67] ArsTechnica, Does Tor provide more benefit or harm? New paper says it depends https://arstechnica.com/gadgets/2020/11/does-tor-provide-more-benefit-or-harm-new-paper-says-it-depends/ [Archive org]

[68] ResearchGate, The potential harms of the Tor anonymity network cluster disproportionately in free countries https://www.pnas.org/content/early/2020/11/24/2011893117 [Archive.org]

[69] CryptoEngineering, How does Apple (privately) find your offline devices? https://blog.cryptographyengineering.com/2019/06/05/how-does-apple-privately-find-your-offline-devices/ [Archive.org]

[70] Apple Support https://support.apple.com/en-us/HT210515 [Archive.org]

[71] XDA, Samsung's Find My Mobile app can locate Galaxy devices even when they're offline https://www.xda-developers.com/samsung-find-my-mobile-app-locate-galaxy-devices-offline/ [Archive.org]

[72] Apple Support, If your Mac is lost or stolen https://support.apple.com/en-us/HT204756 [Archive.org]

Such devices will continue to broadcast identity information to nearby devices even when offline using Bluetooth Low-Energy[73]. They do not have access to the devices directly (which are not connected to the internet) but instead use BLE to find them through other nearby devices[74]. They are basically using peer-to-peer short-range Bluetooth communication to broadcast their status through nearby online devices.

They could now locate such devices and keep the location in some database that could then be used by third parties or themselves for various purposes (including analytics, advertising or evidence/intelligence gathering).

See Appendix N: Warning about smartphones and smart devices

Your Hardware Identifiers:

Your IMEI and IMSI (and by extension, your phone number):

The IMEI (International Mobile Equipment Identity[75]) and the IMSI (International Mobile Subscriber Identity[76]) are unique numbers created by mobile phone manufacturers and mobile phone operators.

The IMEI is tied directly to the phone you are using. This number is known and tracked by the mobile phone operators and known by the manufacturers. Every time your phone connects to the mobile network, it will register the IMEI on the network along the IMSI (if a SIM card is inserted but that is not even needed). It is also used by many applications (Banking apps abusing the phone permission on Android for instance[77]) and smartphone Operating Systems (Android/IOS) for identification of the device[78]. It is possible but difficult (and not illegal in many jurisdictions[79]) to change the IMEI on a phone but it is probably easier and cheaper to just find and buy some old (working) Burner phone for a few Euros (this guide is for Germany remember) at a flea market or at some random small shop.

The IMSI is tied directly to the mobile subscription or pre-paid plan you are using and is basically tied to your phone number by your mobile provider. The IMSI is hardcoded directly on the SIM card and cannot be changed. Remember that every time your phone connects to the mobile network, it will also register the IMSI on the network along the IMEI. Like the IMEI, the IMSI is also being used by some applications and smartphone Operating systems for identification and are being tracked. Some countries in the EU for instance maintain a database of IMEI/IMSI associations for easy querying by Law Enforcement.

Today, giving away your (real) phone number is basically the same or better than giving away your Social Security number/Passport ID/National ID.

The IMEI and IMSI can be traced back to you by at least 6 ways:

- The mobile operator subscriber logs which will usually store the IMEI along the IMSI and their subscriber information database. If you use a prepaid anonymous SIM (anonymous IMSI but with a known IMEI), they can see this cell belongs to you if you used that cell phone before with a different SIM card (different anonymous IMSI but same known IMEI).
- The mobile operator antenna logs which will conveniently keep a log of which IMEI and IMSI also keep some connection data. They know and log for instance that a phone with this IMEI/IMSI combination connected to a set of Mobile antennas and how powerful the signal to each of those antennas was allowing easy triangulation/geolocation of the signal. They also know which other phones (your real one for instance) connected at the same time to the same antennas with the same signal which would make it possible to know precisely that this "burner phone" was always connected at the same place/time than this other

---

[73] Wikipedia, BLE https://en.wikipedia.org/wiki/Bluetooth_Low_Energy [Wikiless] [Archive.org]

[74] Cryptography Engineering Blog, How does Apple (privately) find your offline devices? https://blog.cryptographyengineering.com/2019/06/05/how-does-apple-privately-find-your-offline-devices/ [Archive.org]

[75] Wikipedia, IMEI https://en.wikipedia.org/wiki/International_Mobile_Equipment_Identity [Wikiless] [Archive.org]

[76] Wikipedia, IMSI https://en.wikipedia.org/wiki/International_mobile_subscriber_identity [Wikiless] [Archive org]

[77] Android Documentation, Device Identifiers https://source.android.com/devices/tech/config/device-identifiers [Archive.org]

[78] Google Privacy Policy, Look for IMEI https://policies.google.com/privacy/embedded?hl=en-US [Archive.org]

[79] Wikipedia, IMEI and the Law https://en.wikipedia.org/wiki/International_Mobile_Equipment_Identity#IMEI_and_the_law [Wikiless] [Archive.org]

"known phone" which shows up every time the burner phone is being used. This information can be used by various third parties to geolocate/track you quite precisely[80,81].

- The manufacturer of the Phone can trace back the sale of the phone using the IMEI if that phone was bought in a non-anonymous way. Indeed, they will have logs of each phone sale (including serial number and IMEI), to which shop/person it was sold to. And if you are using a phone that you bought online (or from someone that knows you). It can be traced to you using that information. Even if they do not find you on CCTV[82] and you bought the phone cash, they can still find what other phone (your real one in your pocket) was there (in that shop) at that time/date by using the antenna logs.
- The IMSI alone can be used to find you as well because most countries now require customers to provide an ID when buying a SIM card (subscription or pre-paid). The IMSI is then tied to the identity of the buyer of the card. In the countries where the SIM can still be bought with cash (like the UK), they still know where (which shop) it was bought and when. This information can then be used to retrieve information from the shop itself (such as CCTV footage as for the IMEI case). Or again the antenna logs can also be used to figure out which other phone was there at the moment of the sale.
- The smartphone OS makers (Google/Apple for Android/IOs) also keep logs of IMEI/IMSI identifications tied to Google/Apple accounts and which user has been using them. They too can trace back the history of the phone and to which accounts it was tied in the past[83].
- Government agencies around the world interested in your phone number can and do use[84] special devices called "IMSI catchers"[85] like the Stingray[86] or more recently the Nyxcell[87]. These devices can impersonate (to spoof) a cell phone Antenna and force a specific IMSI (your phone) to connect to it to access the cell network. Once they do, they will be able to use various MITM[88] (Man-In-The-Middle Attacks) that will allow them to:
    - Tap your phone (voice calls and SMS).
    - Sniff and examine your data traffic.
    - Impersonate your phone number without controlling your phone.
    - …

Here is also a good YouTube video on this topic: DEFCON Safe Mode - Cooper Quintin - Detecting Fake 4G Base Stations in Real Time https://www.youtube.com/watch?v=siCk4pGGcqA [Invidious]

For these reasons, it is crucial to get dedicated an anonymous phone number and/or an anonymous burner phone with an anonymous pre-paid sim card that are not tied to you in any way (past or present) for conducting sensitive activities (See more practical guidance in Get an anonymous Phone number section).

While there are some smartphones manufacturers like Purism with their Librem series[89] who claim to have your privacy in mind, they still do not allow IMEI randomization which I believe is a key anti-tracking feature that should be provided by such manufacturers. While this measure will not prevent IMSI tracking within the SIM card, it would

---

[80] Bellingcat, The GRU Globetrotters: Mission London https://www.bellingcat.com/news/uk-and-europe/2019/06/28/the-gru-globetrotters-mission-london/ [Archive.org]

[81] Bellingcat,"V" For "Vympel": FSB's Secretive Department "V" Behind Assassination Of Georgian Asylum Seeker In Germany https://www.bellingcat.com/news/uk-and-europe/2020/02/17/v-like-vympel-fsbs-secretive-department-v-behind-assassination-of-zelimkhan-khangoshvili/ [Archive.org]

[82] Wikipedia, CCTV https://en.wikipedia.org/wiki/Closed-circuit_television [Wikiless] [Archive org]

[83] Apple, Transparency Report, Device Requests https://www.apple.com/legal/transparency/device-requests.html [Archive.org]

[84] The Intercept, How Cops Can Secretly Track Your Phone https://theintercept.com/2020/07/31/protests-surveillance-stingrays-dirtboxes-phone-tracking/ [Archive.org]

[85] Wikipedia, IMSI Catcher https://en.wikipedia.org/wiki/IMSI-catcher [Wikiless] [Archive.org]

[86] Wikipedia, Stingray https://en.wikipedia.org/wiki/Stingray_phone_tracker [Wikiless] [Archive.org]

[87] Gizmodo, Cops Turn to Canadian Phone-Tracking Firm After Infamous 'Stingrays' Become 'Obsolete' https://gizmodo.com/american-cops-turns-to-canadian-phone-tracking-firm-aft-1845442778 [Archive.org]

[88] Wikipedia, MITM https://en.wikipedia.org/wiki/Man-in-the-middle_attack [Wikiless] [Archive org]

[89] Purism, Librem 5 https://shop.puri.sm/shop/librem-5/ [Archive.org]

at least allow you to keep the same "burner phone" and only switch SIM cards instead of having to switch both for privacy.

See Appendix N: Warning about smartphones and smart devices

Your Wi-Fi or Ethernet MAC address:

The MAC address[90] is a unique identifier tied to your physical Network Interface (Wired Ethernet or Wi-Fi) and could of course be used to track you if it is not randomized. As it was the case with the IMEI, manufacturers of computers and network cards usually keep logs of their sales (usually including things like: Serial number, IMEI, Mac Addresses, …) and it is possible again for them to track where and when the computer with the MAC address in question was sold and to whom. Even if you bought it with cash in a supermarket, the supermarket might still have CCTV (or a CCTV just outside that shop) and again the time/date of sale could be used to find out who was there using the Mobile Provider antenna logs at that time (IMEI/IMSI).

Operating Systems makers (Google/Microsoft/Apple) will also keep logs of devices and their MAC addresses in their logs for device identification (Find my device type services for example). Apple can tell that the MacBook with this specific MAC address was tied to a specific Apple Account before. Maybe yours before you decided to use the MacBook for sensitive activities. Maybe to a different user who sold it to you but remembers your e-mail/number from when the sale happened.

Your home router/Wi-Fi access point keeps logs of devices that registered on the Wi-Fi and these can be accessed too to find out who has been using your Wi-Fi. Sometimes this can be done remotely (and silently) by the ISP depending if that router/Wi-Fi access point is being "managed" remotely by the ISP (which is often the case when they provide the router to their customers).

Some commercial devices will keep record of MAC addresses roaming around for various purposes such as road congestion[91].

So, it is important again not to bring your phone along when/where you conduct sensitive activities. If you use your own laptop, then it is crucial to hide that MAC address (and Bluetooth address) anywhere you use it and be extra careful not to leak any information. Thankfully many recent OSes now feature or allow the option to randomize MAC addresses (Android, IOS, Linux and Windows 10) with the notable exception of MacOS which does not support this feature even in its latest Big Sur version.

See Appendix N: Warning about smartphones and smart devices

Your Bluetooth MAC address:

Your Bluetooth MAC is like the previous MAC address except it is for Bluetooth. Again, it can be used to track you as manufacturers and operating system makers keep logs of such information. It could be tied to a sale place/time/date or accounts and then could be used to track you with such information, the shop billing information, the CCTV, or the mobile antenna logs in correlation.

Operating systems have protections in place to randomize those addresses but are still subject to vulnerabilities[92].

For this reason, and unless you really need those, you should just disable Bluetooth completely in the BIOS/UEFI settings if possible or in the Operating System otherwise.

On Windows 10, you will need to disable and enable the Bluetooth device in the device manager itself to force a randomization of the address for next use and prevent tracking.

See Appendix N: Warning about smartphones and smart devices

---

[90] Wikipedia, MAC Address https://en.wikipedia.org/wiki/MAC_address [Wikiless] [Archive org]

[91] Acyclica Road Trend Product Sheet, https://amsignalinc.com/data-sheets/Acyclica/Acyclica-RoadTrend-Product-Sheet.pdf [Archive org]

[92] ResearchGate, Tracking Anonymized Bluetooth Devices https://www.researchgate.net/publication/334590931_Tracking_Anonymized_Bluetooth_Devices/fulltext/5d3308db92851cd04675a469/Tracking-Anonymized-Bluetooth-Devices.pdf [Archive.org]

Your CPU:

All modern CPUs[93] are now integrating hidden management platforms such as the now infamous Intel Management Engine[94] and the AMD Platform Security Processor[95].

Those management platforms are basically small operating systems running directly on your CPU as long as they have power. These systems have full access to your computer's network and could be accessed by an adversary to de-anonymize you in various ways (using direct access or using malware for instance) as shown in this enlightening video: BlackHat, How to Hack a Turned-Off Computer, or Running Unsigned Code in Intel Management Engine https://www.youtube.com/watch?v=mYsTBPqbya8 [Invidious].

These have already been affected by several security vulnerabilities in the past[96] that allowed malware to gain control of target systems. These are also accused by many privacy actors including the EFF and Libreboot of being a backdoor into any system[97].

There are some not so easy ways[98] to disable the Intel IME on some CPUs and you should do so if you can. For some AMD laptops, you can disable it within the BIOS settings by disabling PSP.

Note that to AMD's defense, so far and AFAIK, there were no security vulnerabilities found for ASP and no backdoors eithers: See https://www.youtube.com/watch?v=bKH5nGLgi08&t=2834s [Invidious]. In addition, AMD PSP does not provide any remote management capabilities contrary to Intel IME.

If you are feeling a bit more adventurous, you could install your own BIOS using Libreboot[99] or Coreboot[264] if your laptop supports it (be aware that Coreboot does contain some propriety code unlike its fork Libreboot).

In addition, some CPUs have unfixable flaws (especially Intel CPUs) that could be exploited by various malware. Here is a good current list of such vulnerabilities affecting recent widespread CPUs:

https://en.wikipedia.org/wiki/Transient_execution_CPU_vulnerability [Wikiless] [Archive.org]

- If you are using Linux you can check the vulnerability status of your CPU to Spectre/Meltdown attacks by using https://github.com/speed47/spectre-meltdown-checker [Archive.org] which is available as a package for most Linux distros including Whonix.
- If you are using Windows, you can check the vulnerability status of your CPU using inSpectre https://www.grc.com/inspectre.htm [Archive org]

Some of these can be avoided using Virtualization Software settings that can mitigate such exploits. See this guide for more information https://www.whonix.org/wiki/Spectre_Meltdown [Archive.org] (warning: these can severely impact the performance of your VMs).

I will therefore mitigate some of these issues in this guide by recommending the use of virtual machines on a dedicated anonymous laptop for your sensitive activities that will only be used from an anonymous public network.

Your Operating Systems and Apps telemetry services:

Whether it is Android, iOS, Windows, MacOS or even Ubuntu. Most popular Operating Systems now collect telemetry information by default even if you never opt-in or opted-out[102] from the start. Some like Windows will not

---

[93] Wikipedia, CPU https://en.wikipedia.org/wiki/Central_processing_unit [Wikiless] [Archive.org]

[94] Wikipedia, Intel Management Engine https://en.wikipedia.org/wiki/Intel_Management_Engine [Wikiless] [Archive.org]

[95] Wikipedia, AMD Platform Security Processor https://en.wikipedia.org/wiki/AMD_Platform_Security_Processor [Wikiless] [Archive org]

[96] Wikipedia, IME, Security Vulnerabilities https://en.wikipedia.org/wiki/Intel_Management_Engine#Security_vulnerabilities [Wikiless] [Archive.org]

[97] Wikipedia, IME, Assertions that ME is a backdoor https://en.wikipedia.org/wiki/Intel_Management_Engine#Assertions_that_ME_is_a_backdoor [Wikiless] [Archive.org]

[98] Wikipedia, IME, Disabling the ME https://en.wikipedia.org/wiki/Intel_Management_Engine#Disabling_the_ME [Wikiless] [Archive org]

[99] Libreboot, https://libreboot.org/ [Archive.org]

even allow disabling telemetry completely without some technical tweaks. This information collection can be extensive and include a staggering number of details (metadata and data) on your devices and their usage.

Here are good overviews of what is being collected by those 5 popular OSes in their last versions:

- Android/Google:
  - Just have a read at their privacy policy https://policies.google.com/privacy [Archive.org]
  - School of Computer Science & Statistics, Trinity College Dublin, Ireland Mobile Handset Privacy: Measuring The Data iOS and Android Send to Apple And Google https://www.scss.tcd.ie/doug.leith/apple_google.pdf [Archive.org]
- IOS/Apple:
  - More information at https://www.apple.com/legal/privacy/en-ww/ [Archive.org] and https://support.apple.com/en-us/HT202100 [Archive.org]
  - School of Computer Science & Statistics, Trinity College Dublin, Ireland Mobile Handset Privacy: Measuring The Data iOS and Android Send to Apple And Google https://www.scss.tcd.ie/doug.leith/apple_google.pdf [Archive.org]
  - Apple does claim[100] that they anonymize this data using differential privacy[101] but you will have to trust them on that.
- Windows/Microsoft:
  - Full list of required diagnostic data: https://docs.microsoft.com/en-us/windows/privacy/required-windows-diagnostic-data-events-and-fields-2004 [Archive.org]
  - Full list of optional diagnostic data: https://docs.microsoft.com/en-us/windows/privacy/windows-diagnostic-data [Archive.org]
- MacOS:
  - More details on https://support.apple.com/guide/mac-help/share-analytics-information-mac-apple-mh27990/mac [Archive.org]
- Ubuntu:
  - Ubuntu despite being a Linux distribution also collects Telemetry Data nowadays. This data however is quite limited compared to the others. More details on https://ubuntu.com/desktop/statistics [Archive org]

Not only are Operating Systems gathering telemetry services but so are Apps themselves like Browsers, Mail Clients, and Social Networking Apps installed on your system.

It is important to understand that this telemetry data can be tied to your device and help de-anonymizing you and subsequently can be used against you by an adversary that would get access to this data.

This does not mean for example that Apple devices are terrible choices for good Privacy but they certainly not the best choices for (relative) Anonymity. They might protect you from third parties knowing what you are doing but not from themselves. In all likelihood, they certainly know who you are.

Later in this guide, we will use all the means at our disposal to disable and block as much telemetry as possible to mitigate this attack vector in the Operating Systems supported in this guide.

See Appendix N: Warning about smartphones and smart devices

Your Smart devices in general:

You got it; your smartphone is an advanced spying/tracking device that:

- Records everything you say at any time ("Hey Siri", "Hey Google").
- Records your location everywhere you go.
- Always records other devices around you (Bluetooth devices, Wi-Fi Access points).
- Records your habits and health data (steps, screen time, exposure to diseases, connected devices data)

---

[100] Apple, Differential Privacy White Paper https://www.apple.com/privacy/docs/Differential_Privacy_Overview.pdf [Archive.org]

[101] Wikipedia, Differential Privacy https://en.wikipedia.org/wiki/Differential_privacy [Wikiless] [Archive org]

- Records all your network locations.
- Records all your pictures and videos (and most likely where they were taken).
- Has most likely access to most of your known accounts including social media, Messaging and Financial accounts.

Data is being transmitted even if you opt-out[102], processed, and stored indefinitely (most likely unencrypted[103]) by various third parties[104].

But that is not all, this section is not called "Smartphones" but "Smart devices" because it is not only your smartphone spying on you. It is also every other smart device you could have.

- Your Smart Watch? (Apple Watch, Android Smartwatch …)
- Your Fitness Devices and Apps[105]? (Strava[106,107], Fitbit[108], Garmin, Polar[109], …)
- Your Smart Speaker? (Amazon Alexa[110], Google Echo, Apple Homepod …)
- Your Smart Transportation? (Car? Scooter?)
- Your Smart Tags? (Apple AirTag, Galaxy SmartTag, Tile…)
- Your Car? (Yes, most modern cars have advanced logging/tracking features these days[111])
- Any other Smart device? There are even convenient search engines dedicated to finding them online:
    - https://www.shodan.io/
    - https://censys.io/
    - https://www.zoomeye.org/

See Appendix N: Warning about smartphones and smart devices

Yourself:

Your Metadata including your Geo-Location:

Your metadata is all the information about your activities without the actual content of those activities. For instance, it is like knowing you had a call from an oncologist before then calling your family and friends successively. You do not know what was said during the conversation but you can guess what it was just from the metadata[112].

---

[102] Trinity College Dublin, Mobile Handset Privacy: Measuring The Data iOS and Android Send to Apple And Google https://www.scss.tcd.ie/doug.leith/apple_google.pdf [Archive.org]

[103] Reuters, Exclusive: Apple dropped plan for encrypting backups after FBI complained – sources https://www.reuters.com/article/us-apple-fbi-icloud-exclusive-idUSKBN1ZK1CT [Archive.org]

[104] ZDnet, I asked Apple for all my data. Here's what was sent back https://www.zdnet.com/article/apple-data-collection-stored-request/ [Archive.org]

[105] De Correspondent, Here's how we found the names and addresses of soldiers and secret agents using a simple fitness app https://decorrespondent.nl/8481/heres-how-we-found-the-names-and-addresses-of-soldiers-and-secret-agents-using-a-simple-fitness-app/412999257-6756ba27 [Archive.org]

[106] Wired, The Strava Heat Map and the End of Secrets https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/ [Archive org]

[107] Bellingcat, How to Use and Interpret Data from Strava's Activity Map https://www.bellingcat.com/resources/how-tos/2018/01/29/strava-interpretation-guide/ [Archive.org]

[108] The Guardian, Fitness tracking app Strava gives away location of secret US army bases https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases [Archive.org]

[109] Telegraph, Running app reveals locations of secret service agents in MI6 and GCHQ https://www.telegraph.co.uk/technology/2018/07/08/running-app-exposes-mi6-gchq-workers-whereabouts/ [Archive org]

[110] Washington Post, Alexa has been eavesdropping on you this whole time https://www.washingtonpost.com/technology/2019/05/06/alexa-has-been-eavesdropping-you-this-whole-time/?itid=lk_interstitial_manual_59 [Archive.org]

[111] Washington Post, What does your car know about you? We hacked a Chevy to find out https://www.washingtonpost.com/technology/2019/12/17/what-does-your-car-know-about-you-we-hacked-chevy-find-out/ [Archive org]

[112] Using Metadata to find Paul Revere (https://kieranhealy.org/blog/archives/2013/06/09/using-metadata-to-find-paul-revere/ [Archive org])

This metadata will also often include your location that is being harvested by Smartphones, Operating Systems (Android[113]/IOS), Browsers, Apps, Websites. Odds are there are several companies knowing exactly where you are at any time[114] because of your smartphone[115].

This location data has been used in many judicial cases[116] already as part of "geofence warrants" [117] that allows law enforcement to ask companies (such as Google/Apple) a list of all devices present at a certain location at a certain time. In addition, this location data is even sold by private companies to the military who can then use it conveniently[118].

Now let us say you are using a VPN to hide your IP. The social media platform knows you were active on that account on November 4th from 8am to 1pm with that VPN IP. The VPN allegedly keeps no logs and cannot trace back that VPN IP to your IP. Your ISP however knows (or at least can know) you were connected to that same VPN provider on November 4th from 7:30am to 2pm but does not know what you were doing with it.

The question is: Is there someone somewhere that would possibly have both pieces of information available[119] for correlation in a convenient database?

Have you heard of Edward Snowden[120]? Now is the time to google him and read his book[121]. Also read about XKEYSCORE[122,123], MUSCULAR[124], SORM[125], Tempora[126] and PRISM[127].

See "We kill people based on Metadata"[128] or this famous tweet from the IDF https://twitter.com/idf/status/1125066395010699264 [Archive.org] [Nitter].

See Appendix N: Warning about smartphones and smart devices

Your Digital Fingerprint, Footprint, and Online Behavior:

This is the part where you should watch the documentary "The Social Dilemma"[129] on Netflix as they cover this topic much better than anyone else IMHO.

---

[113] Wikipedia, Google SensorVault, https://en.wikipedia.org/wiki/Sensorvault [Wikiless] [Archive.org]

[114] NRKBeta, My Phone Was Spying on Me, so I Tracked Down the Surveillants https://nrkbeta.no/2020/12/03/my-phone-was-spying-on-me-so-i-tracked-down-the-surveillants/ [Archive org]

[115] New York Times https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html [Archive.org]

[116] Sophos, Google data puts innocent man at the scene of a crime https://nakedsecurity.sophos.com/2020/03/10/google-data-puts-innocent-man-at-the-scene-of-a-crime/ [Archive.org]

[117] Wikipedia, Geofence Warrant https://en.wikipedia.org/wiki/Geo-fence_warrant [Wikiless] [Archive.org]

[118] Vice.com, Military Unit That Conducts Drone Strikes Bought Location Data From Ordinary Apps https://www.vice.com/en/article/y3g97x/location-data-apps-drone-strikes-iowa-national-guard [Archive.org]

[119] Wikipedia, Room 641A https://en.wikipedia.org/wiki/Room_641A [Wikiless] [Archive.org]

[120] Wikipedia, Edward Snowden https://en.wikipedia.org/wiki/Edward_Snowden [Wikiless] [Archive org]

[121] Wikipedia, Permanent Record https://en.wikipedia.org/wiki/Permanent_Record_(autobiography) [Wikiless] [Archive.org]

[122] Wikipedia, XKEYSCORE https://en.wikipedia.org/wiki/XKeyscore [Wikiless] [Archive.org]

[123] ElectroSpaces, Danish military intelligence uses XKEYSCORE to tap cables in cooperation with the NSA https://www.electrospaces.net/2020/10/danish-military-intelligence-uses.html [Archive.org]

[124] Wikipedia, MUSCULAR https://en.m.wikipedia.org/wiki/MUSCULAR_(surveillance_program) [Archive.org]

[125] Wikipedia, SORM https://en.wikipedia.org/wiki/SORM [Wikiless] [Archive.org]

[126] Wikipedia, Tempora https://en.wikipedia.org/wiki/Tempora [Wikiless] [Archive org]

[127] Wikipedia, PRISM https://en.wikipedia.org/wiki/PRISM_(surveillance_program) [Wikiless] [Archive.org]

[128] Justsecurity, General Hayden https://www.justsecurity.org/10318/video-clip-director-nsa-cia-we-kill-people-based-metadata/ [Archive.org]

[129] IDMB, The Social Dilemma https://www.imdb.com/title/tt11464826/ [Archive.org]

This includes is the way you write (stylometry) [130, 131], the way you behave [132, 133]. The way you click. The way you browse. The fonts you use on your browser[134]. Fingerprinting is being used to guess who someone is by the way that user is behaving. You might be using specific pedantic words or making specific spelling mistakes that could give you away using a simple Google search for similar features because you typed in a similar way on some Reddit post 5 years ago using a not so anonymous Reddit account[135].

Social Media platforms such as Facebook/Google can go a step further and can register your behavior in the browser itself. For instance, they can register everything you type even if you do not send it / save it. Think of when you write an e-mail in Gmail. It is saved automatically as you type. They can register your clicks and cursor movements as well.

All they need to achieve this in most cases is Javascript enabled in your Browser (which is the case in most Browsers including Tor Browser by default).

While these methods are usually used for marketing purposes and advertising, they can also be a useful tool for fingerprinting users. This is because your behavior is most likely quite unique or unique enough that over time, you could be de-anonymized.

Here are some examples:

- For example, as a basis of authentication, a user's typing speed, keystroke depressions, patterns of error (say accidentally hitting an "l" instead of a "k" on three out of every seven transactions) and mouse movements establishes that person's unique pattern of behavior[136]. Some commercial services such as TypingDNA (https://www.typingdna.com/ [Archive org]) even offer such analysis as a replacement for two factor authentications.
- This technology is also widely used in CAPTCHAS[327] services to verify that you are "human" and can be used to fingerprint a user.

Analysis algorithms could then be used to match these patterns with other users and match you to a different known user. It is unclear if such data is already used or not by Governments and Law Enforcements agencies but it might be in the future. And while this is mostly used for advertising/marketing/captchas purposes now. It could and probably will be used for investigations in the short or mid-term future to deanonymize users.

Here is a fun example you try yourself to see some of those things in action: https://clickclickclick.click (no archive links for this one sorry). You will see it becoming interesting over time (this requires Javascript enabled).

Here is also a recent example just showing what Google Chrome collects on you: https://web.archive.org/web/https://pbs.twimg.com/media/EwiUNH0UYAgLY7V?format=jpg&name=4096x4096

Here are some other resources on topic if you cannot see this documentary:

- 2017, Behavior Analysis in Social Networks, https://link.springer.com/10.1007/978-1-4614-7163-9_110198-1 [Archive org]

---

[130] ArsTechnica, How the way you type can shatter anonymity—even on Tor https://arstechnica.com/information-technology/2015/07/how-the-way-you-type-can-shatter-anonymity-even-on-tor/ [Archive.org]

[131] Wikipedia, Stylometry https://en.wikipedia.org/wiki/Stylometry [Wikiless] [Archive.org]

[132] Paul Moore Blog, Behavioral Profiling: The password you can't change. https://paul.reviews/behavioral-profiling-the-password-you-cant-change/ [Archive org]

[133] Wikipedia, Sentiment Analysis, https://en.wikipedia.org/wiki/Sentiment_analysis [Wikiless] [Archive.org]

[134] EFF CoverYourTracks, https://coveryourtracks.eff.org/ [Archive.org]

[135] Berkeley.edu, On the Feasibility of Internet-Scale Author Identification https://people.eecs.berkeley.edu/~dawnsong/papers/2012%20On%20the%20Feasibility%20of%20Internet-Scale%20Author%20Identification.pdf [Archive.org]

[136] SecuredTouch Blog, Behavioral Biometrics 101: Behavioral Biometrics vs. Behavioral Analytics https://blog.securedtouch.com/behavioral-biometrics-101-an-in-depth-look-at-behavioral-biometrics-vs-behavioral-analytics [Archive org]

- 2017, Social Networks and Positive and Negative Affect https://www.sciencedirect.com/science/article/pii/S1877042811013747/pdf?md5=253d8f1bb615d5dee195d353dc077d46&pid=1-s2.0-S1877042811013747-main.pdf [Archive.org]
- 2015, Using Social Networks Data for Behavior and Sentiment Analysis https://www.researchgate.net/publication/300562034_Using_Social_Networks_Data_for_Behavior_and_Sentiment_Analysis [Archive.org]
- 2016, A Survey on User Behavior Analysis in Social Networks https://www.academia.edu/30936118/A_Survey_on_User_Behaviour_Analysis_in_Social_Networks [Archive org]
- 2019, Influence and Behavior Analysis in Social Networks and Social Media https://sci-hub.do/10.1007/978-3-030-02592-2 [Archive.org]

So, how can you mitigate this these?

- This guide will provide some technical mitigations using Fingerprinting resistant tools but those might not be sufficient.
- You should apply common sense and try to identify your own patterns in your behavior and behave differently when using anonymous identities. This includes:
    - The way you type (speed, accuracy…).
    - The words you use (be careful with your usual expressions).
    - The type of response you use (if you are sarcastic by default, try to have a different approach with your identities).
    - The way you use your mouse and click (try to solve the Captchas differently than your usual way)
    - The habits you have when using some Apps or visiting some Websites (do not always use the same menus/buttons/links to reach your content).
    - …

Basically, you need to act and fully adopt a role as an actor would do for a performance. You need to become a different person, think, and act like that person. This is not a technical mitigation but a human one. You can only rely on yourself for that.

Ultimately, this is mostly up to you to fool those algorithms by adopting new habits and not revealing real information when using your anonymous identities.

Your Clues about your Real Life and OSINT:

These are clues you might give over time that could point to your real identity. You might be talking to someone or posting on some board/forum/Reddit. In those posts you might over time leak some information about your real life. These might be memories, experiences or clues you shared that could then allow a motivated adversary to build a profile to narrow their search.

A real use and well-documented case of this was the arrest of the hacker Jeremy Hammond[137] who shared over time several details about his past and was later discovered.

There are also a few cases involving OSINT at Bellingcat[138].Have a look at their very informative (but slightly outdated) toolkit here: https://docs.google.com/spreadsheets/d/18rtqh8EG2q1xBo2cLNyhIDuK9jrPGwYr9DI2UncoqJQ/edit#gid=930747607 [Archive org]

You can also view some convenient lists of some available OSINT tools here if you want to try them on yourself for example:

[137] ArsTechnica, Stakeout: how the FBI tracked and busted a Chicago Anon https://arstechnica.com/tech-policy/2012/03/stakeout-how-the-fbi-tracked-and-busted-a-chicago-anon/ [Archive.org]

[138] Bellingcat MH17 - Russian GRU Commander 'Orion' Identified as Oleg Ivannikov https://www.bellingcat.com/news/uk-and-europe/2018/05/25/mh17-russian-gru-commander-orion-identified-oleg-ivannikov/ [Archive org]

- https://github.com/jivoi/awesome-osint [Archive.org]
- https://jakecreps.com/tag/osint-tools/ [Archive org]
- https://osintframework.com/
- https://recontool.org
- https://github.com/jivoi/awesome-osint [Archive.org]

As well as this interesting Playlist on YouTube:
https://www.youtube.com/playlist?list=PLrFPX1Vfqk3ehZKSFeb9pVIHqxqrNW8Sy [Invidious]

As well as those interesting podcasts:

https://www.inteltechniques.com/podcast.html

You should never ever share real personal experiences/details using your anonymous identities that could later lead to finding your real identity.

Your Face, Voice, Biometrics and Pictures:

"Hell is other people", even if you evade every method listed above, you are not out of the woods yet thanks to the widespread use of advanced Face recognition by everyone.

Companies like Facebook have used advanced face recognition for years[139,140] and have been using other means (Satellite imagery) to create maps of "people" around the world[141]. This evolution has been going on for years to the point we can now say "We lost control of our faces"[142].

If you are walking in a touristy place, you will most likely appear in someone's selfie within minutes without knowing it. That person will then proceed to upload that selfie to various platforms (Twitter, Google Photos, Instagram, Facebook, Snapchat …). Those platforms will then apply face recognition algorithms to those pictures under the pretext of allowing better/easier tagging or to better organize your photo library. In addition to this, the same picture will provide a precise timestamp and in most cases geolocation of where it was taken. Even if the person does not provide a timestamp and geolocation, it can still be guessed with other means[143,144].

Here are a few resources for even trying this yourself:

- Bellingcat, Guide To Using Reverse Image Search For Investigations: https://www.bellingcat.com/resources/how-tos/2019/12/26/guide-to-using-reverse-image-search-for-investigations/ [Archive.org]
- Bellingcat, Using the New Russian Facial Recognition Site SearchFace https://www.bellingcat.com/resources/how-tos/2019/02/19/using-the-new-russian-facial-recognition-site-searchface-ru/ [Archive.org]
- Bellingcat, Dali, Warhol, Boshirov: Determining the Time of an Alleged Photograph from Skripal Suspect Chepiga https://www.bellingcat.com/resources/how-tos/2018/10/24/dali-warhol-boshirov-determining-time-alleged-photograph-skripal-suspect-chepiga/ [Archive.org]
- Bellingcat, Advanced Guide on Verifying Video Content https://www.bellingcat.com/resources/how-tos/2017/06/30/advanced-guide-verifying-video-content/ [Archive.org]

---

[139] Facebook Research, Deepface https://research.fb.com/publications/deepface-closing-the-gap-to-human-level-performance-in-face-verification/ [Archive.org]

[140] Privacy News Online, Putting the "face" in Facebook: how Mark Zuckerberg is building a world without public anonymity https://www.privateinternetaccess.com/blog/putting-face-facebook-mark-zuckerberg-building-world-without-public-anonymity/ [Archive.org]

[141] CNBC, "Facebook has mapped populations in 23 countries as it explores satellites to expand internet" https://www.cnbc.com/2017/09/01/facebook-has-mapped-human-population-building-internet-in-space.html [Archive.org]

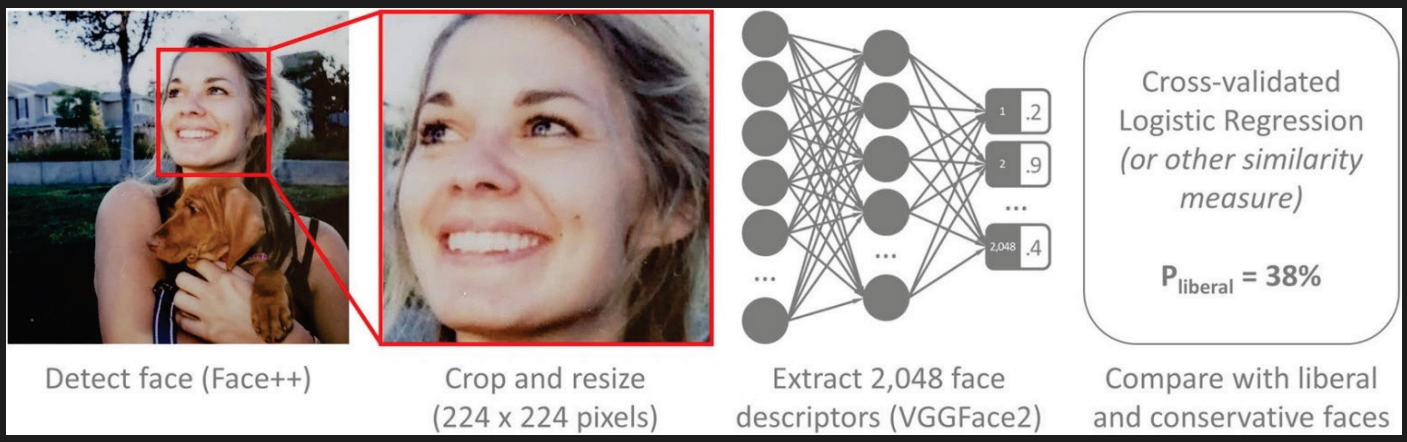
[142] MIT Technology Review, This is how we lost control of our faces, https://www.technologyreview.com/2021/02/05/1017388/ai-deep-learning-facial-recognition-data-history/ [Archive.org]

[143] Bellingcat, Shadow of a Doubt: Crowdsourcing Time Verification of the MH17 Missile Launch Photo https://www.bellingcat.com/resources/case-studies/2015/08/07/shadow-of-a-doubt/ [Archive.org]

[144] Brown Institute, Open-Source Investigation, https://brown.columbia.edu/open-source-investigation/ [Archive.org]

- Bellingcat, Using the Sun and the Shadows for Geolocation https://www.bellingcat.com/resources/2020/12/03/using-the-sun-and-the-shadows-for-geolocation/ [Archive org]
- Bellingcat, Navalny Poison Squad Implicated in Murders of Three Russian Activists https://www.bellingcat.com/news/uk-and-europe/2021/01/27/navalny-poison-squad-implicated-in-murders-of-three-russian-activists/ [Archive org]
- Bellingcat, Berlin Assassination: New Evidence on Suspected FSB Hitman Passed to German Investigators https://www.bellingcat.com/news/2021/03/19/berlin-assassination-new-evidence-on-suspected-fsb-hitman-passed-to-german-investigators/ [Archive org]
- Bellingcat, Digital Research Tutorial: Investigating a Saudi-Led Coalition Bombing of a Yemen Hospital https://www.youtube.com/watch?v=cAVZaPiVArA [Invidious]
- Bellingcat, Digital Research Tutorial: Using Facial Recognition in Investigations https://www.youtube.com/watch?v=awY87q2Mr0E [Invidious]
- Bellingcat, Digital Research Tutorial: Geolocating (Allegedly) Corrupt Venezuelan Officials in Europe https://www.youtube.com/watch?v=bS6gYWM4kzY [Invidious]

Even if you are not looking at the camera, they can still figure out who you are[145], make out your emotions[146], analyze your gait[147] and probably guess your political affiliation[148,149].



Those platforms (Google/Facebook) already know who you are for a few reasons:

- Because you have or had a profile with them and you identified yourself.
- Even if you never made a profile on those platforms, you still have one without even knowing it[150,151,152,153,154].

---

[145] NewScientist, Facebook can recognize you in photos even if you're not looking https://www.newscientist.com/article/dn27761-facebook-can-recognise-you-in-photos-even-if-youre-not-looking/ [Archive.org]

[146] Google Patent, Techniques for emotion detection and content delivery https://patents.google.com/patent/US20150242679 [Archive org]

[147] APNews, Chinese 'gait recognition' tech IDs people by how they walk https://apnews.com/article/bf75dd1c26c947b7826d270a16e2658a [Archive org]

[148] TechCrunch, Facial recognition reveals political party in troubling new research https://techcrunch.com/2021/01/13/facial-recognition-reveals-political-party-in-troubling-new-research/ [Archive.org]

[149] Nature.com, Facial recognition technology can expose political orientation from naturalistic facial images https://www.nature.com/articles/s41598-020-79310-1 [Archive.org]

[150] Slate https://slate.com/technology/2018/04/facebook-collects-data-on-non-facebook-users-if-they-want-to-delete-it-they-have-to-sign-up.html [Archive.org]

[151] The Conversation https://theconversation.com/shadow-profiles-facebook-knows-about-you-even-if-youre-not-on-facebook-94804 [Archive.org]

[152] The Verge https://www.theverge.com/2018/4/11/17225482/facebook-shadow-profiles-zuckerberg-congress-data-privacy [Archive org]

[153] ZDNET https://www.zdnet.com/article/anger-mounts-after-facebooks-shadow-profiles-leak-in-bug/ [Archive org]

[154] CNET https://www.cnet.com/news/shadow-profiles-facebook-has-information-you-didnt-hand-over/ [Archive.org]

- Because other people have tagged you or identified you in their holidays/party pictures.
- Because other people have put a picture of you in their contact list which they then shared with them.

Here is also an insightful demo of Microsoft Azure you can try for yourself at https://azure.microsoft.com/en-us/services/cognitive-services/face/#demo where you can detect emotions and compare faces from different pictures.

Governments already know who you are because they have your ID/Passport/Driving License pictures and often added biometrics (Fingerprints) in their database. Those same governments are integrating those technologies (often provided by private companies such as the Israeli AnyVision[155], Clearview AI[156], or NEC[157]) in their CCTV networks to look for "persons of interest"[158]. And some heavily surveilled states like China have implemented widespread use of Facial Recognition for various purposes[159] including possibly identifying ethnic minorities[160]. A simple face recognition error by some algorithm can ruin your life[161].

Here are some resources detailing some techniques used by Law Enforcement today:

- CCC video explaining current Law Enforcement surveillance capabilities: https://media.ccc.de/v/rc3-11406-spot_the_surveillance#t=761 [Archive.org]
- EFF SLS: https://www.eff.org/sls [Archive.org]

Apple is making FaceID mainstream and pushing its use it to log you in in various services including the Banking systems.

Same goes with fingerprint authentication being mainstreamed by many smartphone makers to authenticate yourself. A simple picture where your fingers appear can be used to de-anonymize you[162,163,164].

Same goes with your voice which can be analyzed by for various purposes as shown in the recent Spotify patent[165].

We can safely imagine a near future where you will not be able to create accounts or sign-in anywhere without providing unique biometrics (A good time to re-watch Gattaca[166], Person of Interest[167] and Minority Report[168]). And you can safely imagine how useful these large biometrics databases could be to some interested third parties.

---

[155] Anyvision https://www.anyvision.co/ [Archive org]

[156] BuzzFeed.news, Surveillance Nation https://www.buzzfeednews.com/article/ryanmac/clearview-ai-local-police-facial-recognition [Archive.org]

[157] NEC, Neoface https://www.nec.com/en/global/solutions/biometrics/face/neofacewatch.html [Archive.org]

[158] The Guardian, Met police deploy live facial recognition technology https://www.theguardian.com/uk-news/2020/feb/11/met-police-deploy-live-facial-recognition-technology [Archive.org]

[159] YouTube, The Economist, China: facial recognition and state control https://www.youtube.com/watch?v=lH2gMNrUuEY [Invidious]

[160] Washington Post, Huawei tested AI software that could recognize Uighur minorities and alert police, report says https://www.washingtonpost.com/technology/2020/12/08/huawei-tested-ai-software-that-could-recognize-uighur-minorities-alert-police-report-says/ [Archive.org]

[161] The Intercept, How a Facial Recognition Mismatch Can Ruin Your Life https://theintercept.com/2016/10/13/how-a-facial-recognition-mismatch-can-ruin-your-life/ [Archive.org]

[162] BBC, WhatsApp photo drug dealer caught by 'groundbreaking' work https://www.bbc.com/news/uk-wales-43711477 [Archive org]

[163] CNN, Drug dealer jailed after sharing a photo of cheese that included his fingerprints https://edition.cnn.com/2021/05/25/uk/drug-dealer-cheese-sentenced-scli-gbr-intl/index.html [Archive.org]

[164] Vice.com, Cops Got a Drug Dealer's Fingerprints From Photos of His Hand on WhatsApp https://www.vice.com/en/article/evqk9e/photo-of-fingerprints-used-to-arrest-drug-dealers [Archive.org]

[165] JUSTIA Patent, Identification of taste attributes from an audio signal https://patents.justia.com/patent/10891948 [Archive.org]

[166] IMDB, Gattaca 1997, https://www.imdb.com/title/tt0119177/ [Archive.org]

[167] IMDB, Person of Interest 2011 https://www.imdb.com/title/tt1839578 [Archive.org]

[168] IMDB, Minority Report 2002, https://www.imdb.com/title/tt0181689 [Archive.org]

In addition, all this information can also be used against you (if you are already de-anonymized) using deepfake[169] by crafting false information (Pictures, Videos, Voice Recordings[170]…) and have already been used for such purposes[171,172]. There are even commercial services for this readily available such as https://www.respeecher.com/ [Archive org] and https://www.descript.com/overdub [Archive org].

See this demo: https://www.youtube.com/watch?v=t5yw5cR79VA [Invidious]

At this time, there are a few steps[173] you can use to mitigate (and only mitigate) face recognition when conducting sensitive activities where CCTV might be present:

- Wear a facemask as they have been proven to defeat some face recognition technologies[174] but not all[175].
- Wear a baseball cap or hat to mitigate identification from high angle CCTVs (filming from above) from recording your face. Remember this will not help against front-facing cameras.
- Wear sunglasses in addition to the facemask and baseball cap to mitigate identification from your eye's features.
- Consider wearing special sunglasses (expensive unfortunately) called "Reflectacles" https://www.reflectacles.com/ [Archive org]. There was a small study showing their efficiency against IBM and Amazon facial recognition[176].

(Note that if you intend to use these where advanced facial recognition systems have been installed, these measures could also flag as you as suspicious by themselves and trigger a human check)

Phishing and Social Engineering:

Phishing[177] is a social engineering[178] type of attack where an adversary could try to extract information from you by pretending or impersonating something/someone else.

A typical case is an adversary using a man-in-the-middle[88] attack or a fake e-mail/call to ask your credential for a service. This could for example be through e-mail or through impersonating financial services.

Such attacks can also be used to de-anonymize someone by tricking them into downloading malware or revealing personal information over time.

These have been used countless times since the early days of the internet and the usual one is called the "419 scam" (see https://en.wikipedia.org/wiki/Advance-fee_scam [Wikiless] [Archive.org]).

Here is a good video if you want to learn a bit more about phishing types: Black Hat, Ichthyology: Phishing as a Science https://www.youtube.com/watch?v=Z20XNp-IuNA [Invidious].

---

[169] Wikipedia, Deepfake https://en.wikipedia.org/wiki/Deepfake [Wikiless] [Archive.org]

[170] Econotimes, Deepfake Voice Technology: The Good. The Bad. The Future https://www.econotimes.com/Deepfake-Voice-Technology-The-Good-The-Bad-The-Future-1601278 [Archive.org]

[171] Wikipedia, Deepfake Events https://en.wikipedia.org/wiki/Deepfake#Example_events [Wikiless] [Archive.org]

[172] Forbes, A Voice Deepfake Was Used To Scam A CEO Out Of $243,000 https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/ [Archive.org]

[173] Joseph Steinberg, How To Prevent Facial Recognition Technology From Identifying You https://josephsteinberg.com/how-to-prevent-facial-recognition-technology-from-identifying-you/ [Archive.org]

[174] NIST, Face recognition accuracy with masks using pre-COVID-19 algorithms https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8311.pdf [Archive.org]

[175] BBC, Facial recognition identifies people wearing masks https://www.bbc.com/news/technology-55573802 [Archive.org]

[176] University of Wisconsin, Exploring Reflectacles As Anti-Surveillance Glasses and for Adversarial Machine Learning in Computer Vision http://diglib.uwgb.edu/digital/api/collection/p17003coll4/id/71/download [Archive.org]

[177] Wikipedia, Phishing https://en.wikipedia.org/wiki/Phishing [Wikiless] [Archive.org]

[178] Wikipedia, Social Engineering https://en.wikipedia.org/wiki/Social_engineering_(security) [Wikiless] [Archive.org]

Malware, exploits, and viruses:

Malware in your files/documents/e-mails:

Using steganography or other techniques, it is easy to embed malware into common file formats such as Office Documents, Pictures, Videos, PDF documents…

These can be as simple as HTML tracking links or complex targeted malware.

These could be simple pixel sized images[179] hidden in your e-mails that would call a remote server to try and get your IP address.

These could be exploiting a vulnerability in an outdated format or outdated reader. Such exploits could then be used to compromise your system.

See these good videos for more explanations on the matter:

- What is a File Format? https://www.youtube.com/watch?v=VVdmmN0su6E [Invidious]
- Ange Albertini: Funky File Formats: https://www.youtube.com/watch?v=hdCs6bPM4is [Invidious]

You should always use extreme caution. To mitigate these attacks, this guide will later recommend the use of virtualization (See Appendix W: Virtualization) to mitigate leaking any information even in case of opening such a malicious file.

If you want to learn how to try detecting such malware, see Appendix T: Checking files for malware

Malware and Exploits in your apps and services:

So, you are using Tor Browser or Brave Browser over Tor. You could be using those over a VPN for added security. But you should keep in mind that there are exploits[180] (hacks) that could be known by an adversary (but unknown to the App/Browser provider). Such exploits could be used to compromise your system and reveal details to de-anonymize you such as your IP address or other details.

A real use case of this technique was the Freedom Hosting[181] case in 2013 where the FBI inserted malware[182] using a Firefox browser exploit on a Tor website. This exploit allowed them to reveal details of some users. More recently, there was the notable SolarWinds[183] hack that breached several US government institutions by inserting malware into an official software update server.

In some countries, Malware is just mandatory and/or distributed by the state itself. This is the case for instance in China with WeChat[184] which can then be used in combination with other data for state surveillance[185].

There are countless examples of malicious browser extensions, smartphone apps and various apps that have been infiltrated with malware over the years.

Here are some steps to mitigate this type of attack:

- You should never have 100% trust in the apps you are using.
- You should always check that you are using the updated version of such apps before use and ideally validate each download using their signature if available.

---

[179] BBC, Spy pixels in emails have become endemic https://www.bbc.com/news/technology-56071437 [Archive.org]

[180] Wikipedia, Exploit https://en.wikipedia.org/wiki/Exploit_(computer_security) [Wikiless] [Archive.org]

[181] Wikipedia, Freedom Hosting https://en.wikipedia.org/wiki/Freedom_Hosting [Wikiless] [Archive org]

[182] Wired, 2013 FBI Admits It Controlled Tor Servers Behind Mass Malware Attack https://www.wired.com/2013/09/freedom-hosting-fbi/ [Archive.org]

[183] Wikipedia, 2020 United States federal government data breach https://en.wikipedia.org/wiki/2020_United_States_federal_government_data_breach [Wikiless] [Archive.org]

[184] BBC, China social media: WeChat and the Surveillance State https://www.bbc.com/news/blogs-china-blog-48552907 [Archive org]

[185] The Intercept, Revealed: Massive Chinese Police Database https://theintercept.com/2021/01/29/china-uyghur-muslim-surveillance-police/ [Archive.org]

- You should not use such apps directly from a hardware system but instead use a Virtual Machine for compartmentalization.

To reflect these recommendations, this guide will therefore later guide you in the use of Virtualization (See Appendix W: Virtualization) so that even if your Browser/Apps get compromised by a skilled adversary, that adversary will find himself stuck in a sandbox[186] without being able to access identifying information, or compromise your system.

Malicious USB devices:

There are readily available commercial and cheap "badUSB" [187]devices that can take deploy malware, log your typing, geolocate you, listen to you or gain control of your laptop just by plugging them in. Here are some examples that you can already buy yourself.

- Hak5, USB Rubber Ducky https://shop.hak5.org/products/usb-rubber-ducky-deluxe [Archive.org]
- Hak5, O.MG Cable https://www.youtube.com/watch?v=V5mBJHotZv0 [Invidious]
- Keelog https://www.keelog.com/ [Archive.org]
- AliExpress https://www.aliexpress.com/i/4000710369016.html [Archive.org]

Such devices can be implanted anywhere (charging cable, mouse, keyboard, USB key …) by an adversary and can be used to track you or compromise your computer or smartphone. The most notable example of such attacks is probably Stuxnet[188] in 2005.

While you could inspect an USB key physically, scan it with various utilities, check the various components to see if they are genuine, you will most likely never be able to discover complex malware embedded in genuine parts of a genuine USB key by a skilled adversary without advanced forensics equipment[189].

To mitigate this, you should never trust such devices and plug them into sensitive equipment. If you use a charging device, you should consider the use of an USB data blocking device that will only allow charging but not any data transfer. Such data blocking devices are now readily available in many online shops. You should also consider disabling USB ports completely within the BIOS of your computer unless you need them (if you can).

Malware and backdoors in your Hardware Firmware and Operating System:

This might sound a bit familiar as this was already partially covered previously in the Your CPU section.

Malware and backdoors can be embedded directly into your hardware components. Sometimes those backdoors are implemented by the manufacturer itself such as the IME in the case of Intel CPUs. And in other cases, such backdoors can be implemented by a third party that places itself between orders of new hardware and customer delivery[190].

Such malware and backdoors can also be deployed by an adversary using software exploits. Many of those are called rootkits[191] within the tech world. Usually, these types of malwares are harder to detect and mitigate as they are implemented at a lower level than the userspace[192] and often in the firmware[193] of hardware components itself.

---

[186] Wikipedia, Sandbox https://en.wikipedia.org/wiki/Sandbox_(computer_security) [Wikiless] [Archive org]

[187] Wired, Why the Security of USB Is Fundamentally Broken https://www.wired.com/2014/07/usb-security/ [Archive.org]

[188] Wikipedia, Stuxnet https://en.wikipedia.org/wiki/Stuxnet [Wikiless] [Archive.org]

[189] Superuser.com, How do I safely investigate a USB stick found in the parking lot at work? https://superuser.com/questions/1206321/how-do-i-safely-investigate-a-usb-stick-found-in-the-parking-lot-at-work [Archive.org]

[190] The Guardian, Glenn Greenwald: how the NSA tampers with US-made internet routers https://www.theguardian.com/books/2014/may/12/glenn-greenwald-nsa-tampers-us-internet-routers-snowden [Archive.org]

[191] Wikipedia, Rootkit https://en.wikipedia.org/wiki/Rootkit [Wikiless] [Archive.org]

[192] Wikipedia, Userspace https://en.wikipedia.org/wiki/User_space [Wikiless] [Archive.org]

[193] Wikipedia, Firmware https://en.wikipedia.org/wiki/Firmware [Wikiless] [Archive.org]

What is firmware? Firmware is a low-level operating system for devices. Each component in your computer probably has firmware including for instance your disk drives. The BIOS[194]/UEFI[195] system of your machine for instance is a type of firmware.

These can allow remote management and capable of enabling full control on a target system silently and stealthily.

As mentioned previously, these are harder to detect by users but nevertheless some limited steps that can be taken to mitigate some those by protecting your device from tampering and use some measures (like re-flashing the bios for example). Unfortunately, if such malware or backdoor is implemented by the manufacturer itself, it becomes extremely difficult to detect and disable those.

Your files, documents, pictures, and videos:

Properties and Metadata:

This can be obvious to many but not to all. Most files have metadata attached to them. A good example are pictures which store EXIF[196] information which can contain a lot of information such as GPS coordinates, which camera/phone model took it and when it was taken precisely. While this information might not directly give out who you are, it could tell exactly where you were at a certain moment which could allow others to use different sources to find you (CCTV or other footage taken at the same place at the same time during a protest for instance). It is important that you verify any file you would put on those platforms for any properties that might contain any information that might lead back to you.

Here is an example of EXIF data that could be on a picture:

Global Positioning System	
GPS Altitude	31.9 m
GPS Latitude	6deg 14' 7.620"
GPS Longitude	106deg 49' 30.210"
Image Information	
Date and Time	2018:08:24 15:47:27
Manufacturer	Apple
Model	iPhone 6s
Photograph Information	
Aperture	F2.2
Exposure Bias	0 EV
Exposure Mode	Auto
Exposure Program	Auto
Exposure Time	1/874 s
Flash	No, auto
FNumber	F2.2
Focal Length	4.2 mm
ISO Speed Ratings	25
Metering Mode	Multi-segment
Shutter speed	1/874 s
White Balance	Auto

[194] Wikipedia, BIOS https://en.wikipedia.org/wiki/BIOS [Wikiless] [Archive org]

[195] Wikipedia, UEFI https://en.wikipedia.org/wiki/Unified_Extensible_Firmware_Interface [Wikiless] [Archive.org]

[196] Bellingcat, Joseph Mifsud: Rush for the EXIF https://www.bellingcat.com/news/americas/2018/10/26/joseph-mifsud-rush-exif/ [Archive.org]

(Illustration from Wikipedia)

By the way, this also works for videos. Yes, videos too have geo-tagging and many are very unaware of this. Here Is for instance a very convenient tool to geo-locate YouTube videos: https://mattw.io/youtube-geofind/location [Archive org]

For this reason, you will always have to be very careful when uploading files using your anonymous identities and check the metadata of those files.

Even if you publish a simple text file, you should always double or triple check it for any information leakage before publishing. You will find some guidance about this in the Some additional measures against forensics section at the end of the guide.

Watermarking:

Pictures/Videos/Audio:

Pictures/Videos often contain visible watermarks indicating who is the owner/creator but there are also invisible watermarks in various products aiming at identifying the viewer itself.

So, if you are a whistleblower and thinking about leaking some picture/audio/video file. Think twice. There are chances that those might contain invisible watermarking within them that would include information about you as a viewer. Such watermarks can be enabled with a simple switch in like Zoom (Video[197] or Audio[198]) or with extensions[199] for popular apps such as Adobe Premiere Pro. These can be inserted by various content management systems.

For a recent example where someone leaking a Zoom meeting recording was caught because it was watermarked: https://theintercept.com/2021/01/18/leak-zoom-meeting/ [Archive.org]

Such watermarks can be inserted by various products[200, 201, 202, 203] using Steganography[204] and can resist compression[205] and re-encoding[206, 207].

These watermarks are not easily detectable and could allow identification of the source despite all efforts.

In addition to watermarks, the camera used for filming (and therefore the device used for filming) a video can also be identified using various techniques such as lens identification[208] which could lead to de-anonymization.

Be extremely careful when publishing videos/pictures/audio files from known commercial platforms as they might contain such invisible watermarks in addition to details in the images themselves.

---

[197] Zoom Support, Adding a watermark https://support.zoom.us/hc/en-us/articles/209605273-Adding-a-Watermark [Archive.org]

[198] Zoom Support, Audio Watermark https://support.zoom.us/hc/en-us/articles/360021839031-Audio-Watermark [Archive.org]

[199] CreativeCloud Extension, IMATAG https://exchange.adobe.com/creativecloud.details.101789.imatag-invisible-watermark-and-image-monitoring.html [Archive.org]

[200] NexGuard, https://dtv.nagra.com/nexguard-forensic-watermarking [Archive.org]

[201] Vobile Solutions, https://www.vobilegroup.com/solutions [Archive.org]

[202] Cinavia, https://www.cinavia.com/languages/english/pages/technology.html [Archive.org]

[203] Imatag, https://www.imatag.com/ [Archive.org]

[204] Wikipedia, Steganography https://en.wikipedia.org/wiki/Steganography [Wikiless] [Archive.org]

[205] IEEExplore, A JPEG compression resistant steganography scheme for raster graphics images https://ieeexplore.ieee.org/document/4428921 [Archive org]

[206] ScienceDirect, Robust audio watermarking using perceptual masking https://www.sciencedirect.com/science/article/abs/pii/S0165168498000140 [Archive org]

[207] IEEExplore, Spread-spectrum watermarking of audio signals https://ieeexplore.ieee.org/abstract/document/1188746 [Archive org]

[208] Google Scholar, source camera identification https://scholar.google.com/scholar?q=source+camera+identification [Archive.org]

Printing Watermarking:

Did you know your printer is most likely spying on you too? Even if it is not connected to any network? This is usually a known fact by many people in the IT community but few outside people.

Yes … Your printers can be used to de-anonymize you as well as explained by the EFF here https://www.eff.org/issues/printers [Archive.org]

With this (old but still relevant) video explaining how from the EFF as well: https://www.youtube.com/watch?v=izMGMsIZK4U [Invidious]

Basically, many printers will print an invisible watermark allowing for identification of the printer on every printed page. This is called Printer Steganography[209].There is no real way to mitigate this but to inform yourself on your printer and make sure it does not print any invisible watermark. This is obviously important if you intend to print anonymously.

Here is an (old but still relevant) list of printers and brands who do not print such tracking dots provided by the EFF https://www.eff.org/pages/list-printers-which-do-or-do-not-display-tracking-dots [Archive.org]

Here are also some tips from the Whonix documentation (https://www.whonix.org/wiki/Printing_and_Scanning [Archive org]):

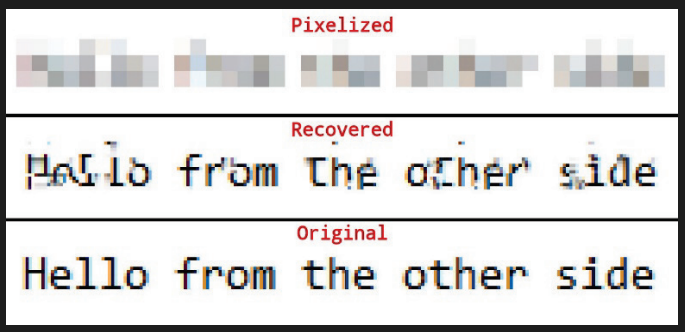
Do not ever print in Color, usually watermarkings are not present without color toners/cartridges[210].

Pixelized or Blurred Information:

Did you ever see a document with blurred text? Did you ever make fun of those movies/series where they "enhance" an image to recover seemingly impossible to read information?

Well, there are techniques for recovering information from such documents, videos, and pictures.

Here is for example an open-source project you could use yourself for recovering text from some blurred images yourself: https://github.com/beurtschipper/Depix [Archive.org]

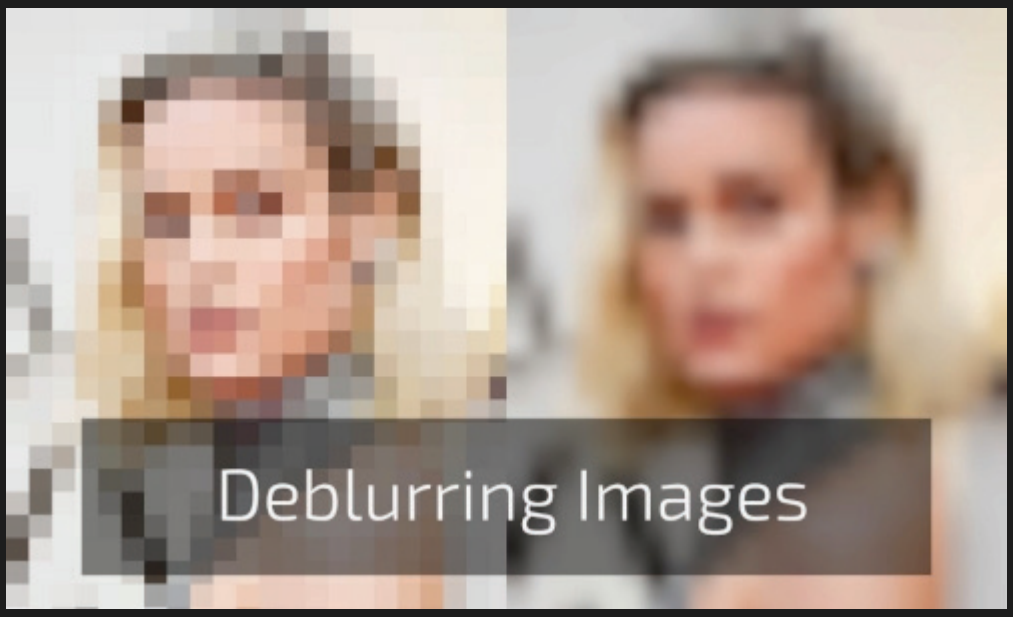


This is of course an open-source project available for all to use. But you can probably imagine that such techniques have probably been used before by other adversaries. These could be used to reveal blurred information from published documents that could then be used to de-anonymize you.

There are also tutorials for using such techniques using Photo Editing tools such as GIMP such as: https://medium.com/@somdevsangwan/unblurring-images-for-osint-and-more-part-1-5ee36db6a70b [Archive.org] followed by https://medium.com/@somdevsangwan/deblurring-images-for-osint-part-2-ba564af8eb5d [Archive.org]

[209] Wikipedia, Printing Steganography https://en.wikipedia.org/wiki/Machine_Identification_Code [Wikiless] [Archive org]

[210] MIT, SeeingYellow, http://seeingyellow.com/ [Archive.org]

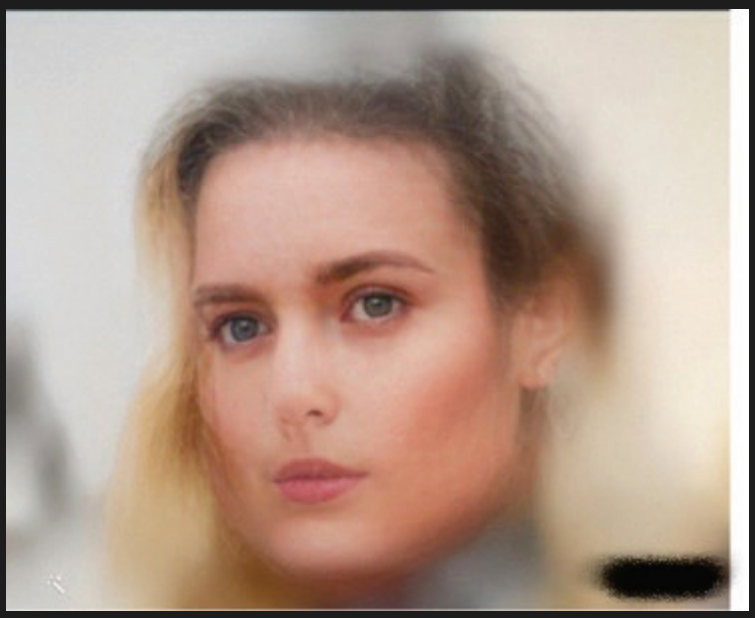


Finally, you will find plenty of deblurring resources here: https://github.com/subeeshvasu/Awesome-Deblurring [Archive org]

Some online services could even help you do this automatically to some extent like MyHeritage.com enhance tool:

https://www.myheritage.com/photo-enhancer [Archive org]

Here is the result of the above image:



Of course, this tool is more like "guessing" than really deblurring at this point but it could be enough to find you using various reverse image searching services.

For this reason, it is always extremely important that you correctly redact and curate any document you might want to publish. Blurring is not enough and you should always completely blacken/remove any sensitive data to avoid any attempt at recovering data from any adversary.

Your Crypto currencies transactions:

Contrary to popular belief, Crypto transactions (such as Bitcoin and Ethereum) are not anonymous[211]. Most crypto currencies can be tracked accurately through various methods[212].

Remember what they say on their own page: https://bitcoin.org/en/you-need-to-know [Archive.org] and https://bitcoin.org/en/protect-your-privacy [Archive.org].

"Bitcoin is not anonymous "

The main issue is not setting up a random Crypto wallet to receive some currency behind a VPN/Tor address (at this point, the wallet is anonymous). The issue is mainly when you want to convert Fiat money (Euros, Dollars …) to Crypto and then when you want to cash in your Crypto. You will have few realistic options but to transfer those to an exchange (such as Coinbase/Kraken/Bitstamp/Binance). Those exchanges have known wallet addresses and will keep detailed logs (due to KYC[213] financial regulations) and can then trace back those crypto transactions to you using the financial system[214].

There are some crypto currencies with privacy/anonymity in mind like Monero but even those have some and warnings to consider[215,216].

Even if you use Mixers or Tumblers[217] (services that specialize in "anonymizing" crypto currencies by "mixing them"), keep in mind this is only obfuscation[218] and not actual anonymity[219]. Not only are they only obfuscation but they could also put you in trouble as you might end up exchanging your crypto against "dirty" crypto that was used in various questionable contexts[220].

This does not mean you cannot use Bitcoin anonymously at all. You can actually use Bitcoin anonymously as long as you do not convert it to actual currency and use a Bitcoin wallet from a safe anonymous network. Meaning you should avoid KYC/AML regulations by various exchanges and avoid using the Bitcoin network from any known IP address. See Appendix Z: Paying anonymously online with BTC.

Overall, IMHO, the best option for using Crypto with reasonable anonymity and privacy is still Monero and you should ideally not use any other for sensitive transactions unless you are aware of the limitations and risks involved. Please do read this Monero Disclaimer.

Your Cloud backups/sync services:

All companies are advertising their use of end-to-end encryption (E2EE). This is true for almost every messaging app and website (HTTPS). Apple and Google are advertising their use of encryption on their Android devices and their iPhones.

But what about your backups? Those automated iCloud/google drive backups you have?

Well, you should probably know that most of those backups are not fully end to end encrypted and will contain some of your information readily available for a third party. You will see their claims that data is encrypted at rest

---

[211] arXiv, An Analysis of Anonymity in the Bitcoin System https://arxiv.org/abs/1107.4524 [Archive org]

[212] Bellingcat, How To Track Illegal Funding Campaigns Via Cryptocurrency, https://www.bellingcat.com/resources/how-tos/2019/03/26/how-to-track-illegal-funding-campaigns-via-cryptocurrency/ [Archive.org]

[213] Wikipedia, KYC https://en.wikipedia.org/wiki/Know_your_customer [Wikiless] [Archive org]

[214] arXiv.org, Probing the Mystery of Cryptocurrency Theft: An Investigation into Methods for Taint Analysis https://arxiv.org/pdf/1906.05754.pdf [Archive.org]

[215] YouTube, Breaking Monero https://www.youtube.com/watch?v=WOyC6OB6ezA&list=PLsSYUeVwrHBnAUre2G_LYDsdo-tD0ov-y [Invidious]

[216] Monero, Monero vs Princeton Researchers, https://monero.org/monero-vs-princeton-researchers/ [Archive.org]

[217] Wikipedia, Cryptocurrency Tumbler https://en.wikipedia.org/wiki/Cryptocurrency_tumbler [Wikiless] [Archive org]

[218] Wikipedia, Security Through Obscurity https://en.wikipedia.org/wiki/Security_through_obscurity [Wikiless] [Archive.org]

[219] ArXiv, Tracking Mixed Bitcoins, https://arxiv.org/abs/2009.14007 [Archive.org]

[220] SSRN, The Cryptocurrency Tumblers: Risks, Legality and Oversight https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3080361 [Archive org]

and safe from anyone … Except they usually do keep a key to access some of the data themselves. These keys are used for them indexing your content, recover your account, collecting various analytics.

There are specialized commercial forensics solutions available (Magnet Axiom[221], Cellebrite Cloud[222]) that will help an adversary analyze your cloud data with ease.

Notable Examples:

- Apple iCloud: https://support.apple.com/en-us/HT202303 [Archive.org] : "Messages in iCloud also uses end-to-end encryption. If you have iCloud Backup turned on**, your backup includes a copy of the key protecting your Messages**. This ensures you can recover your Messages if you lose access to iCloud Keychain and your trusted devices. ".
- Google Drive and WhatsApp: https://faq.whatsapp.com/android/chats/about-google-drive-backups/ [Archive org] : "**Media and messages you back up aren't protected by WhatsApp end-to-end encryption while in Google Drive**. ".
- Dropbox: https://www.dropbox.com/privacy#terms [Archive.org] "To provide these and other features, **Dropbox accesses, stores, and scans Your Stuff**. You give us permission to do those things, and this permission extends to our affiliates and trusted third parties we work with".
- Microsoft OneDrive: https://privacy.microsoft.com/en-us/privacystatement [Archive.org] : Productivity and communications products, "When you use OneDrive, we collect data about your usage of the service, as well as the content you store, to provide, improve, and protect the services. **Examples include indexing the contents of your OneDrive documents so that you can search for them later and using location information to enable you to search for photos based on where the photo was taken**".

You should not trust cloud providers with your (not previously and locally encrypted) sensitive data and you should be wary of their privacy claims. In most cases they can access your data and provide it to a third party if they want to.

The only way to mitigate this is to encrypt yourself your data on your side and then only upload it to such services.

Your Browser and Device Fingerprints:

Your Browser and Device Fingerprints[339] are set of properties/capabilities of your System/Browser. These are used on most websites for invisible user tracking but also to adapt the website user experience depending on their browser. For instance, websites will be able to provide a "mobile experience" if you are using a mobile browser or propose a specific language/geographic version depending on your fingerprint. Most of those techniques work with recent Browsers like Chromium[223] based browsers (such as Chrome) or Firefox[224] unless taking special measures.

You can find a lot of detailed information and publications about this on these resources:

- https://amiunique.org/links [Archive.org]
- https://brave.com/brave-fingerprinting-and-privacy-budgets/ [Archive.org]

Most of the time, those fingerprints will unfortunately be unique or nearly unique to your Browser/System. This means that even If you log out from a website and then log back in using a different username, your fingerprint might remain the same if you did not take precautionary measures.

An adversary could then use such fingerprints to track you across multiple services even if you have no account on any of them and are using ad blocking. These fingerprints could in turn be used to de-anonymize you if you keep the same fingerprint between services.

---

[221] Magnet Forensics, Magnet AXIOM https://www.magnetforensics.com/products/magnet-axiom/cloud/ [Archive org]

[222] Cellebrite, Unlock cloud-based evidence to solve the case sooner https://www.cellebrite.com/en/ufed-cloud/ [Archive.org]

[223] Chromium Documentation, Technical analysis of client identification mechanisms https://sites.google.com/a/chromium.org/dev/Home/chromium-security/client-identification-mechanisms#TOC-Machine-specific-characteristics [Archive org]

[224] Mozilla Wiki, Fingerprinting https://wiki.mozilla.org/Fingerprinting [Archive.org]

It should also be noted that while some browsers and extensions will offer fingerprint resistance, this resistance in itself can also be used to fingerprint you as explained here https://palant.info/2020/12/10/how-anti-fingerprinting-extensions-tend-to-make-fingerprinting-easier/ [Archive.org]

This guide will mitigate these issues by mitigating, obfuscating, and randomizing many of those fingerprinting identifiers by using Virtualization (See Appendix W: Virtualization) and using by fingerprinting resistant Browsers.

Local Data Leaks and Forensics:

Most of you have probably seen enough Crime dramas on Netflix or TV to know what forensics are. These are technicians (usually working for law enforcement) that will perform various analysis of evidence. This of course could include your smartphone or laptop.

While these might be done by an adversary when you already got "burned", these might also be done randomly during a routine control or a border check. These unrelated checks might reveal secret information to adversaries that had no prior knowledge of such activities.

Forensics techniques are now very advanced and can reveal a staggering amount information from your devices even if they are encrypted[225]. These techniques are widely used by law enforcement all over the world and should be considered.

Here are some recent resources you should read about your smartphone:

- UpTurn, The Widespread Power of U.S. Law Enforcement to Search Mobile Phones https://www.upturn.org/reports/2020/mass-extraction/ [Archive.org]
- New-York Times, The Police Can Probably Break Into Your Phone https://www.nytimes.com/2020/10/21/technology/iphone-encryption-police.html [Archive org]
- Vice, Cops Around the Country Can Now Unlock iPhones, Records Show https://www.vice.com/en/article/vbxxxd/unlock-iphone-ios11-graykey-grayshift-police [Archive org]

I also highly recommend that you read some documents from a forensics examiner perspective such as:

- EnCase Forensic User Guide, http://encase-docs.opentext.com/documentation/encase/forensic/8.07/Content/Resources/External%20Files/EnCase%20Forensic%20v8.07%20User%20Guide.pdf [Archive.org]
- FTK Forensic Toolkit, https://accessdata.com/products-services/forensic-toolkit-ftk [Archive.org]
- SANS Digital Forensics and Incident Response Videos, https://www.youtube.com/c/SANSDigitalForensics/videos

And finally, here is this very instructive detailed paper on the current state of IOS/Android security from the John Hopkins University: https://securephones.io/main.html[226].

When it comes to your laptop, the forensics techniques are many and widespread. Many of those issues can be mitigated by using full disk encryption, virtualization (See Appendix W: Virtualization), and compartmentalization. This guide will later detail such threats and techniques to mitigate them.

Bad Cryptography:

There is a frequent adage among the infosec community: "Don't roll your own crypto!".

[225] Grayshirt, https://www.grayshift.com/ [Archive org]

[226] Securephones.io, Data Security on Mobile Devices: Current State of the Art, Open Problems, and Proposed Solutions https://securephones.io/main.pdf [Archive.org]

And there are reasons[227,228,229] for that:

Personally, I would not want people discouraged from studying and innovating in the crypto field because of that adage. So instead, I would recommend people to be cautious with "Roll your own crypto" because it is not necessarily good crypto.

- Good cryptography is not easy and usually takes years of research to develop and fine-tune.
- Good cryptography is transparent and not proprietary/closed-source so it can be reviewed by peers.
- Good cryptography is developed carefully, slowly, and rarely alone.
- Good cryptography is usually presented and discussed in conferences, and published on various journals.
- Good cryptography is extensively peer reviewed before it is released for use into the wild.
- Using and implementing existing good cryptography correctly is already a challenge.

Yet, this is not stopping some from doing it anyway and publishing various production Apps/Services using their own self-made cryptography or proprietary closed-source methods.

- You should apply caution when using Apps/Services using closed-source or proprietary encryption methods. All the good crypto standards are public and peer reviewed and there should be no issue disclosing the one you use.
- You should be wary of Apps/Services using a "modified" or proprietary cryptographic method[230].
- By default, you should not trust any "Roll your own crypto" until it was audited, peer-reviewed, vetted, and accepted by the cryptography community[231,232].
- There is no such thing as "military grade crypto"[233,234,235].

Cryptography is a complex topic and bad cryptography could easily lead to your de-anonymization.

In the context of this guide, I recommend sticking to Apps/Services using well established, published, and peer reviewed methods.

So, what to prefer and what to avoid as of 2021? You will have to look up for yourself to get the technical details of each app and see if they are using "bad crypto" or "good crypto". Once you get the technical details, you could check this page for seeing what it is worth: https://latacora.micro.blog/2018/04/03/cryptographic-right-answers.html [Archive org]

Here are some examples:

- Hashes:
  - Prefer: SHA256 (widely used), SHA512 (preferred), or SHA-3
  - Avoid: SHA-1, SHA-2, MD5 (unfortunately sill widely used, CRC, MD6 (rarely used)
- File/Disk Encryption:

---

[227] Loup-Vaillant.fr, Rolling Your Own Crypto https://loup-vaillant.fr/articles/rolling-your-own-crypto [Archive org]

[228] Dhole Moments, Crackpot Cryptography and Security Theater https://soatok.blog/2021/02/09/crackpot-cryptography-and-security-theater/ [Archive.org]

[229] Vice.com, Why You Don't Roll Your Own Crypto https://www.vice.com/en/article/wnx8nq/why-you-dont-roll-your-own-crypto [Archive.org]

[230] YouTube, Great Crypto Failures https://www.youtube.com/watch?v=loy84K3AJ5Q [Invidious]

[231] Cryptography Dispatches, The Most Backdoor-Looking Bug I've Ever Seen https://buttondown.email/cryptography-dispatches/archive/cryptography-dispatches-the-most-backdoor-looking/ [Archive.org]

[232] Citizenlab.ca, Move Fast and Roll Your Own Crypto https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/ [Archive.org]

[233] Jack Poon, The myth of military grade encryption https://medium.com/@atcipher/the-myth-of-military-grade-encryption-292313ae6369 [Archive.org]

[234] Congruent Labs, Stop calling it "Military-Grade Encryption" https://blog.congruentlabs.co/military-grade-encryption/ [Archive org]

[235] IronCoreLabs Blog, "Military Grade Encryption" https://blog.ironcorelabs.com/military-grade-encryption-69aae0145588 [Archive org]

    - Prefer:
        - Hardware Accelerated[236]: AES 256 Bits with HMAC-SHA-2 or HMAC-SHA-3 (This is what Veracrypt, Bitlocker, Filevault 2, KeepassXC, and LUKS use)
        - Non-Hardware Accelerated: Same as accelerated above or if available prefer[237] ChaCha20[238] or XChaCha20 (You can use ChaCha20 with Kryptor https://www.kryptor.co.uk, unfortunately it is not available with Veracrypt).
    - Avoid: Pretty much anything else
- Password Storage:
    - Prefer: argon2, scrypt, bcrypt, SHA-3 or if not possible at least PBKDF2 (only as a last resort)
    - Avoid: naked SHA-2, SHA-1, MD5
- Browser Security (HTTPS):
    - Prefer: TLS 1.3 (ideally TLS 1.3 with ECH/eSNI support) or at least TLS 1.2 (widely used)
    - Avoid: Anything Else (TLS =<1.1, SSL =<3)
- Signing with PGP/GPG:
    - Prefer ECDSA (ed25519)+ECDH (ec25519) or RSA 4096 Bits*
    - Avoid: RSA 2048 bits
- SSH keys:
    - ED25519 (preferred) or RSA 4096 Bits*
    - Avoid: RSA 2048 bits

*** Warning: RSA and ED25519 are unfortunately not seen as "Quantum Resistant"[239] and while they have not been broken yet, they probably will be broken someday into the future. It is probably just a matter of when rather than if RSA will ever be broken. So, these are preferred in those contexts due to the lack of a better option.**

Here are some real cases of issues bad cryptography:

- Telegram: https://buttondown.email/cryptography-dispatches/archive/cryptography-dispatches-the-most-backdoor-looking/ [Archive.org]
- Cryptocat: https://web.archive.org/web/20130705051050/https://blog.crypto.cat/2013/07/new-critical-vulnerability-in-cryptocat-details/
- Some other examples can be found here: https://www.cryptofails.com/ [Archive org]

No logging but logging anyway policies:

Many people have the idea that privacy-oriented services such as VPN or E-Mail providers are safe due to their no logging policies or their encryption schemes. Unfortunately, many of those same people forget that all those providers are legal commercial entities subject to the laws of the countries in which they operate.

Any of those providers can be forced to silently (without your knowing (using for example a court order with a gag order[240] or a national security letter[241]) log your activity to de-anonymize you. There have been several recent examples of those:

- 2021, DoubleVPN servers, logs, and account info seized by law enforcement[242]
- 2021, The Germany based mail provider Tutanota was forced to monitor specific accounts for 3 months[243]

---

[236] Wikipedia, AES Instruction Set, https://en.wikipedia.org/wiki/AES_instruction_set [Wikiless] [Archive.org]

[237] GitHub Issues, https://github.com/AnonymousPlanet/thgtoa/issues/36 [Archive org]

[238] Wikipedia, ChaCha Variants, https://en.wikipedia.org/wiki/Salsa20#ChaCha_variant [Wikiless] [Archive.org]

[239] Wikipedia, Shor's Algorithm, https://en.wikipedia.org/wiki/Shor%27s_algorithm [Wikiless] [Archive.org]

[240] Wikipedia, Gag Order, https://en.wikipedia.org/wiki/Gag_order [Wikiless] [Archive.org]

[241] Wikipedia, National Security Letter https://en.wikipedia.org/wiki/National_security_letter [Wikiless] [Archive.org]

[242] BleepingComputer, DoubleVPN servers, logs, and account info seized by law enforcement https://www.bleepingcomputer.com/news/security/doublevpn-servers-logs-and-account-info-seized-by-law-enforcement/ [Archive org]

[243] CyberScoop, Court rules encrypted email provider Tutanota must monitor messages in blackmail case https://www.cyberscoop.com/court-rules-encrypted-email-tutanota-monitor-messages/ [Archive org]

- 2020, The Germany based mail provider Tutanota was forced to implement a backdoor to intercept and save copies of the unencrypted e-mails of one user[244] (they did not decrypt the stored e-mail).
- 2017, PureVPN was forced to disclose information of one user to the FBI[245].
- 2014, EarthVPN user was arrested based on logs provider to the Dutch Police[246].
- 2014, HideMyAss user was de-anonymized and logs were provided to the FBI[247].
- 2013, Secure E-Mail provider Lavabit shuts down after fighting a secret gag order[248].

Some providers have implemented the use of a Warrant Canary[249] that would allow their users to find out if they have been compromised by such orders but this has not been tested yet as far as I know.

Finally, it is now well known that some companies might be sponsored front-ends for some state adversaries (see the Crypto AG story[250] and Omnisec story[251]).

For these reasons, it is important that you do not trust such providers for your privacy despite all their claims. In most cases, you will be the last person to know if any of your account was targeted by such orders and you might never know at all.

To mitigate this, in cases where you want to use a VPN, I will recommend the use of a cash/Monero-paid VPN provider over Tor to prevent the VPN service from knowing any identifiable information about you.

Some Advanced targeted techniques:

(Illustration: excellent movie I highly recommend: Das Leben der Anderen[252])

[244] Heise Online (German), https://www.heise.de/news/Gericht-zwingt-Mailprovider-Tutanota-zu-Ueberwachungsfunktion-4972460.html [Archive org]

[245] PCMag, Did PureVPN Cross a Line When It Disclosed User Information? https://www.pcmag.com/opinions/did-purevpn-cross-a-line-when-it-disclosed-user-information [Archive.org]

[246] Internet Archive, Wipeyourdata, "No logs" EarthVPN user arrested after police finds logs https://archive.is/XNuVw#selection-230.0-230.1 [Archive.org]

[247] Internet Archive, Invisibler, What Everybody Ought to Know About HideMyAss https://archive.is/ag9w4#selection-136.0-136.1 [Archive.org]

[248] Wikipedia, Lavabit Suspension and Gag order, https://en.wikipedia.org/wiki/Lavabit#Suspension_and_gag_order [Wikiless] [Archive org]

[249] Wikipedia, Warrant Canary https://en.wikipedia.org/wiki/Warrant_canary [Wikiless] [Archive.org]

[250] Washington Post, The intelligence coup of the century https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/ [Archive.org]

[251] Swissinfo.ch, Second Swiss firm allegedly sold encrypted spying devices https://www.swissinfo.ch/eng/second-swiss-firm-allegedly-sold-encrypted-spying-devices/46186432 [Archive org]

[252] Wikipedia, Das Leben der Anderen https://en.wikipedia.org/wiki/The_Lives_of_Others [Wikiless] [Archive.org]

There are many advanced techniques that can be used by skilled adversaries[253] to bypass your security measures provided they already know where your devices are. Many of those techniques are detailed here https://cyber.bgu.ac.il/advanced-cyber/airgap [Archive.org] (Air-Gap Research Page, Cyber-Security Research Center, Ben-Gurion University of the Negev, Israel) and include:

- Attacks that require a malware implanted in some device:
  - Exfiltration of Data through a Malware infected Router: https://www.youtube.com/watch?v=mSNt4h7EDKo [Invidious]
  - Exfiltration of Data through observation of Light variation in a Backlit keyboard with a compromised camera: https://www.youtube.com/watch?v=1kBGDHVr7x0 [Invidious]
    - Exfiltration of Data through a compromised Security Camera (that could first use the previous attack) https://www.youtube.com/watch?v=om5fNqKjj2M [Invidious]
    - Communication from outsider to compromised Security Cameras through IR light signals: https://www.youtube.com/watch?v=auoYKSzdOj4 [Invidious]
  - Exfiltration of data from a compromised air-gapped computer through acoustic analysis of the FAN noises with a smartphone https://www.youtube.com/watch?v=v2_sZIfZkDQ [Invidious]
  - Exfiltration of data from a malware infected air-gapped computer through HD Leds with a Drone https://www.youtube.com/watch?v=4vIu8ld68fc [Invidious]
  - Exfiltration of data from a USB malware on an air-gapped computer through electromagnetic interferences https://www.youtube.com/watch?v=E28V1t-k8Hk [Invidious]
  - Exfiltration of data from a malware infected HDD drive through covert acoustic noise https://www.youtube.com/watch?v=H7lQXmSLiP8 [Invidious]
  - Exfiltration of data through GSM frequencies from a compromised (with malware) air-gapped computer https://www.youtube.com/watch?v=RChj7Mg3rC4 [Invidious]
  - Exfiltration of data through electromagnetic emissions from a compromised Display device https://www.youtube.com/watch?v=2OzTWiGl1rM&t=20s [Invidious]
  - Exfiltration of data through magnetic waves from a compromised air-gapped computer to a Smartphone stored inside a Faraday bag https://www.youtube.com/watch?v=yz8E5n1Tzlo [Invidious]
  - Communication between two compromised air-gapped computers using ultrasonic soundwaves https://www.youtube.com/watch?v=yz8E5n1Tzlo [Invidious]
  - Exfiltration of Bitcoin Wallet from a compromised air-gapped computer to a smartphone https://www.youtube.com/watch?v=2WtiHZNeveY [Invidious]
  - Exfiltration of Data from a compromised air-gapped computer using display brightness https://www.youtube.com/watch?v=ZrkZUO2g4DE [Invidious]
  - Exfiltration of Data from a compromised air-gapped computer through vibrations https://www.youtube.com/watch?v=XGD343nq1dg [Invidious]
  - Exfiltration of Data from a compromised air-gapped computer by turning RAM into a Wi-Fi emitter https://www.youtube.com/watch?v=vhNnc0ln63c [Invidious]
  - Exfiltration of Data from a compromised air-gapped computer through power lines https://arxiv.org/abs/1804.04014 [Archive.org]
- **Attacks that require no malware:**
  - Observing a light bulb from a distance to listen to the sound in the room[254] **without any malware**: Demonstration: https://www.youtube.com/watch?v=t32QvpfOHqw [Invidious]

Here is also a good video from the same authors to explain those topics: Black Hat, The Air-Gap Jumpers https://www.youtube.com/watch?v=YKRtFgunyj4 [Invidious]

[253] Wired, Mind the Gap: This Researcher Steals Data With Noise, Light, and Magnets https://www.wired.com/story/air-gap-researcher-mordechai-guri/ [Archive org]

[254] Ben Nassi, Lamphone, https://www.nassiben.com/lamphone [Archive org]

Realistically, this guide will be of little help against such adversaries as these malwares could be implanted on the devices by a manufacturer or anyone in the middle or by anyone with physical access to the air-gapped computer but there are still some ways to mitigate such techniques:

- Do not conduct sensitive activity while connected to an untrusted/unsecure power line to prevent power line leaks.
- Do not use your devices in front of a camera that could be compromised.
- Use your devices in a soundproofed room to prevent sound leaks.
- Use your devices in faraday cage to prevent electromagnetic leaks.
- Do not talk sensitive information where lightbulbs could be observed from outside.
- Buy your devices from different/unpredictable/offline places (shops) where the probability of them being infected with such malware is lower.
- Do not let anyone access your air-gapped computers except trusted people.

Some bonus resources:

- Have a look at the Whonix Documentation concerning Data Collection techniques here: https://www.whonix.org/wiki/Data_Collection_Techniques [Archive.org]
- You might also enjoy looking at this service https://tosdr.org/ [Archive.org] (Terms of Services, Didn't Read) that will give you a good overview of the various ToS of many services.
- Have a look at https://www.eff.org/issues/privacy [Archive.org] for some more resources.
- Have a look at https://en.wikipedia.org/wiki/List_of_government_mass_surveillance_projects [Wikiless] [Archive org] to have an overview of all known mass-surveillance projects, current and past.
- Have a look at https://www.gwern.net/Death-Note-Anonymity [Archive org] (even if you don't know about Death Note).
- Consider finding and reading Michael Bazzell's book "Open Source Intelligence Techniques" (8th edition as of this writing to find out more about recent OSINT techniques) https://inteltechniques.com/book1.html [Archive org]
- Finally, check https://www.freehaven.net/anonbib/date.html [Archive.org] for the latest academic papers related to Online Anonymity.

Notes:

If you still do not think such information can be used by various actors to track you, you can see some statistics for yourself for some platforms and keep in mind those are only accounting for the lawful data requests and will not count things like PRISM, MUSCULAR, SORM or XKEYSCORE explained earlier:

- Google Transparency Report https://transparencyreport.google.com/user-data/overview [Archive org]
- Facebook Transparency Report https://transparency.facebook.com/ [Archive.org]
- Apple Transparency Report https://www.apple.com/legal/transparency/ [Archive org]
- Cloudflare Transparency Report https://www.cloudflare.com/transparency/ [Archive org]
- Snapchat Transparency Report https://www.snap.com/en-US/privacy/transparency [Archive.org]
- Telegram Transparency Report https://t.me/transparency [Archive org] (requires telegram installed)
- Microsoft Transparency Report https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report [Archive.org]
- Amazon Transparency Report https://www.amazon.com/gp/help/customer/display.html?nodeId=GYSDRGWQ2C2CRYEF [Archive.org]
- Dropbox Transparency Report https://www.dropbox.com/transparency [Archive.org]
- Discord Transparency Report https://blog.discord.com/discord-transparency-report-jan-june-2020-2ef4a3ee346d [Archive.org]
- GitHub Transparency Report https://github.blog/2021-02-25-2020-transparency-report/ [Archive.org]
- Snapchat Transparency Report https://www.snap.com/en-US/privacy/transparency/ [Archive.org]
- TikTok Transparency Report https://www.tiktok.com/safety/resources/transparency-report?lang=en [Archive org]
- Reddit Transparency Report https://www.reddit.com/wiki/transparency [Archive.org]

- Twitter Transparency Report https://transparency.twitter.com/ [Archive.org]

General Preparations:

Personally, in the context of this guide, it is also interesting to have a look at your security model. And in this context, I only have one to recommend:

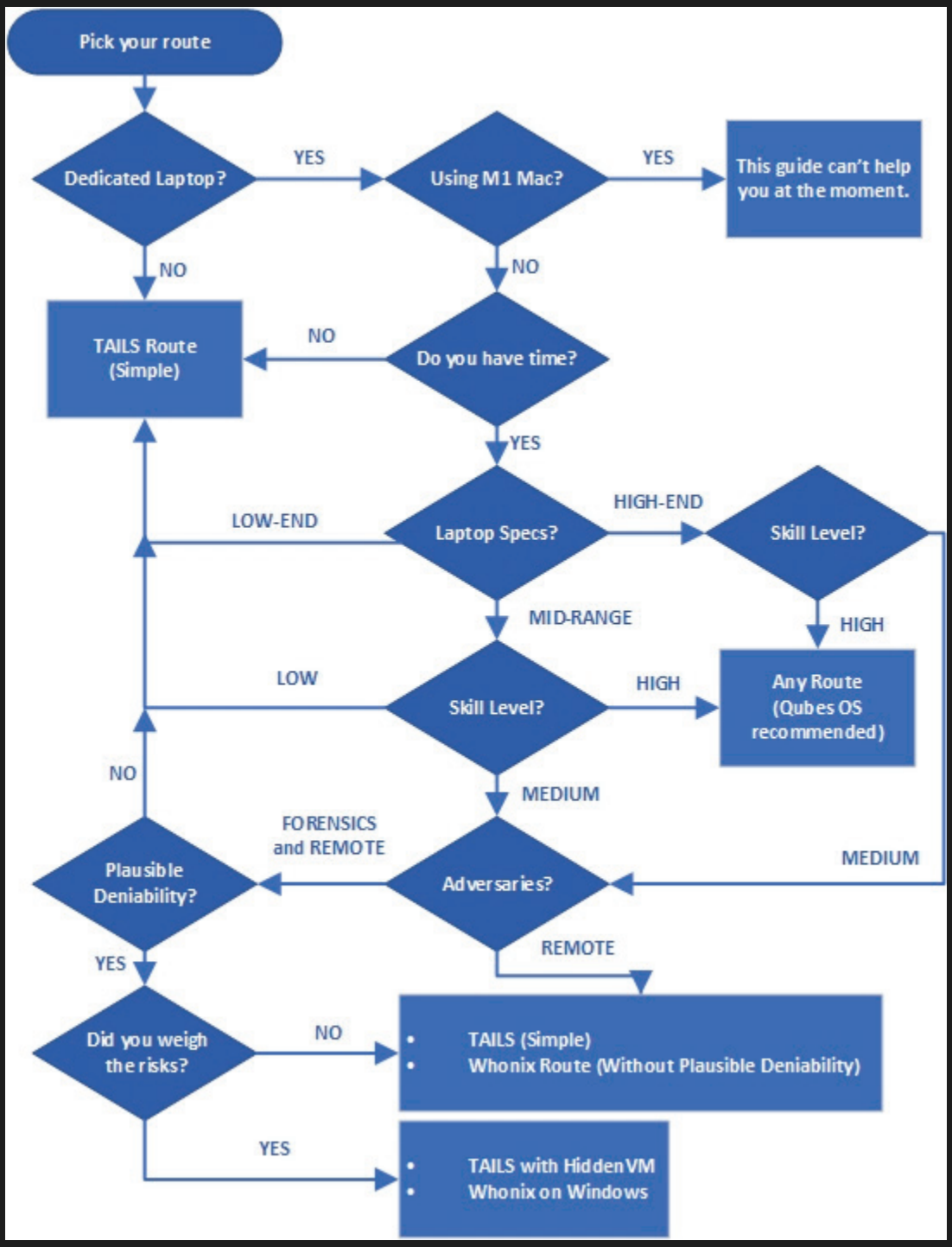
Zero-Trust Security[348] ("Never trust, always verify").

Here are some various resources about what is Zero-Trust Security:

- DEFCON, Zero Trust a Vision for Securing Cloud, https://www.youtube.com/watch?v=euSsqXO53GY [Invidious]
- From the NSA themselves, Embracing a Zero Trust Security Model, https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF [Archive.org]

Picking your route:

Here is a small basic UML diagram showing your options. See the details below.



Timing limitations:

- You have very limited time to learn and need a fast-working solution:
  - **Your best option is to go for the Tails route (excluding the persistent plausible deniability section).**
- You have time and more importantly will to learn:
  - **Go with any route.**

Budget/Material limitations:

- You only have one laptop available and cannot afford anything else. You use this laptop for either work, family, or your personal stuff (or both):
  - **Your best option is to go for the Tails route.**
- You can afford a spare dedicated unsupervised/unmonitored laptop for your sensitive activities:
  - But it is old, slow and has bad specs (less than 6GB of RAM, less than 250GB disk space, old/slow CPU):
    - **You should go for the Tails route.**

- It is not that old and it has decent specs (at least 6GB of RAM, 250GB of disk space or more, decent CPU):
  - **You could go for Tails, Whonix routes.**
- It is new and it has great specs (more than 8GB of RAM, >250GB of disk space, recent fast CPU):
  - **You could go for any route but I would recommend Qubes OS if your threat model allows it.**
- If it is an ARM based M1 Mac:
  - **Not possible currently for these reasons:**
    - **Virtualization of x86 images on ARM M1 Macs is still limited to commercial software (Parallels) which is not supported by Whonix yet.**
    - **Virtualbox is not available for ARM architecture yet.**
    - **Whonix is not supported on ARM architecture yet.**
    - **Tails is not supported on ARM architecture yet.**
    - **Qubes OS is not supported on ARM architecture yet.**

Your only option on M1 Macs is probably to stick with Tor Browses for now. But I would guess that if you can afford an M1 Mac you should probably get a dedicated x86 laptop for more sensitive activities.

Skills:

- You have no IT skills at all the content of this guide looks like an alien language to you?
  - **You should go with the Tails route (excluding the persistent plausible deniability section).**
- You have some IT skills and mostly understand this guide so far
  - **You should go with Tails (including the persistent plausible deniability section) or Whonix routes.**
- You have moderate to high IT skills and you are already familiar with some of the content of this guide
  - **You could go with anything you like but I would strongly recommend Qubes OS.**
- You are a l33T hacker, "there is no spoon", "the cake is a lie", you have been using "doas" for years and "all your base are belong to us", and you have strong opinions on systemd.
  - **This guide is not really meant for you and will not help you with your HardenedBSD on your hardened Libreboot laptop ;-)**

Adversaries (threats):

- If your main concern is forensic examination of your devices:
  - **You should go with the Tails route (with optional persistent plausible deniability).**
- If your main concerns are remote adversaries that might uncover your online identity in various platforms:
  - **You could go with the Whonix or Qubes OS routes.**
  - **You could also go with Tails (with optional persistent plausible deniability).**
- If you absolutely want system wide plausible deniability[272,255] despite the risks[256,275]:
  - **You could go with the Tails Route including the persistent plausible deniability section.**
  - **You could go with the Whonix Route (on Windows Host OS only within the scope of this guide).**
- If you are in a hostile environment where Tor/VPN usage alone is impossible/dangerous/suspicious:
  - **You could go with the Tails route (without using Tor).**
  - **You could go with the Whonix or Qubes OS route (without actually using Whonix).**

In all cases, you should read these two pages from the Whonix documentation that will give you in depth insight about your choices:

- https://www.whonix.org/wiki/Warning [Archive.org]
- https://www.whonix.org/wiki/Dev/Threat_Model [Archive.org]
- https://www.whonix.org/wiki/Comparison_with_Others [Archive org]

[255] Wikipedia, Rubber-hose Cryptanalysis https://en.wikipedia.org/wiki/Rubber-hose_cryptanalysis

[256] Defuse.ca, TrueCrypt's Plausible Deniability is Theoretically Useless https://defuse.ca/truecrypt-plausible-deniability-useless-by-game-theory.htm [Archive.org]

You might be asking yourself: "How do I know if I'm in a hostile online environment where activities are actively monitored and blocked?"

- First read more about it at the EFF here: https://ssd.eff.org/en/module/understanding-and-circumventing-network-censorship [Archive.org]
- Check some data yourself here on the Tor Project OONI[257] (Open Observatory of Network Interference) website: https://explorer.ooni.org/ [Archive.org]
- Have a look at https://censoredplanet.org/ [Archive.org] and see if they have data about your country.
- Test for yourself using OONI (this can be risky in a hostile environment).

Steps for all routes:

Get used to use better passwords:

See Appendix A2: Guidelines for passwords and passphrases.

Get an anonymous Phone number:

Skip this step if you have no intention of creating anonymous accounts on most mainstream platforms but just want anonymous browsing or if the platforms you will use allow registration without a phone number.

Physical Burner Phone and prepaid SIM card:

Get a burner phone:

This is rather easy. Leave your smartphone off or power it off before leaving. Have some cash and go to some random flea market or small shop (ideally one without CCTV inside or outside and while avoiding being photographed/filmed) and just buy the cheapest phone you can find with cash and without providing any personal information. It only needs to be in working order.

Personally, I would recommend getting an old "dumbphone" with a removable battery (old Nokia if your mobile networks still allow those to connect as some countries phased out 1G-2G completely). This is to avoid the automatic sending/gathering of any telemetry/diagnostic data on the phone itself. You should never connect that phone to any Wi-Fi.

It will also be crucial not to power on that burner phone ever (not even without the SIM card) in any geographical location that could lead to you (at your home/work for instance) and never ever at the same location as your other known smartphone (because that one has an IMEI/IMSI that will easily lead to you). This might seem like a big burden but it is not as these phones are only being used during the setup/sign-up process and for verification from time to time.

See Appendix N: Warning about smartphones and smart devices

You should test that the phone is in working order before going to the next step. But I will repeat myself and state again that it is important to leave your smartphone at home when going (or turn it off before leaving if you must keep it) and that you test the phone at a random location that cannot be tracked back to you (and again, do not do that in front of a CCTV, avoid cameras, be aware of your surroundings). No need for Wi-Fi at this place either.

When you are certain the phone is in working order, disable Bluetooth then power it off (remove the battery if you can) and go back home and resume your normal activities. Go to the next step.

Get an anonymous pre-paid SIM card:

This is the hardest part of the whole guide. It is a SPOF (Single Point of Failure). The places where you can still buy prepaid SIM cards without ID registration are getting increasingly limited due to various KYC type regulations[258].

So here is a list of places where you can still get them now: https://prepaid-data-sim-card.fandom.com/wiki/Registration_Policies_Per_Country [Archive.org]

---

[257] Wikipedia, OONI, https://en.wikipedia.org/wiki/OONI [Wikiless] [Archive.org]

[258] Privacy International, Timeline of SIM Card Registration Laws https://privacyinternational.org/long-read/3018/timeline-sim-card-registration-laws [Archive.org]

You should be able to find a place that is "not too far" and just go there physically to buy some pre-paid cards and top-up vouchers with cash. Do verify that no law was passed before going that would make registration mandatory (in case the above wiki was not updated). Try to avoid CCTV and cameras and do not forget to buy a Top Up voucher with the SIM card (if it is not a package) as most pre-paid cards will require a top-up before use.

See Appendix N: Warning about smartphones and smart devices

Double-check that the mobile operators selling the pre-paid SIM cards will accept the SIM activation and top-up without any ID registration of any kind before going there. Ideally, they should accept SIM activation and top-up from the country you reside in.

Personally, I would recommend GiffGaff in the UK as they are "affordable", do not require identification for activation and top-up and will even allow you to change your number up to 2 times from their website. One GiffGaff prepaid SIM card will therefore grant you 3 numbers to use for your needs.

Power off the phone after activation/top-up and before going home. Do not ever power it on again unless you are not at a place that can be used to reveal your identity and unless your smartphone is powered off before going to that "not your home" place.

Online Phone Number (less recommended):

DISCLAIMER: Do not attempt this until you are done setting up a secure environment according to one of the selected routes. This step will require online access and should only be done from an anonymous network. Do not do this from any known/unsecure environment. Skip this until you have finished one of the routes.

There are many commercial services offering numbers to receive SMS messages online but most of those have basically no anonymity/privacy and can be of no help as most Social Media platforms place a limit on how many times a phone number can be used for registration.

There are some forums and subreddits (like r/phoneverification/) where users will offer the service of receiving such SMS messages for you for a small fee (using PayPal or some crypto payment). Unfortunately, these are full of scammer and very risky in terms of anonymity. **You should not use those under any circumstance.**

To this date, I do not know any reputable service that would offer this service and accept cash payments (by post for instance) like some VPN providers. But there are a few services providing online phone numbers and do accept Monero which could be reasonably anonymous (yet less recommended than that physical way in the previous chapter) that you could consider:

- **Recommended**: Do not require any identification (even e-mail):
  - (UK based) https://dtmf.io/ [Archive org] **preferred** because they even provide an onion hidden service address for direct access through the Tor Network at http://dtmfiovjh42uviqez6qn75igbagtiyo724hy3rdxm77dy2m5tt7lbaqd.onion/
  - (Iceland based) https://crypton.sh [Archive org]
  - (Ukraine based) https://virtualsim.net/ [Archive.org]
- Do require identification (valid e-mail):
  - (Germany based) https://www.sms77.io/ [Archive.org]
  - (Russia based) https://onlinesim.ru/ [Archive.org]

There are some other possibilities listed here https://cryptwerk.com/companies/sms/xmr/ [Archive org]. **Use at your own risk.**

DISCLAIMER: I cannot vouch for any of these providers and therefore I will still recommend doing it yourself physically. In this case you will have to rely on the anonymity of Monero and you should not use any service that requires any kind of identification using your real identity. Please do read this Monero Disclaimer.

Therefore IMHO, it is probably just more convenient, cheaper, and less risky to just get a pre-paid SIM card from one of the physical places who still sell them for cash without requiring ID registration. But at least there is an alternative if you have no other option.

Get an USB key:

Get at least one or two decent size generic USB keys (at least 16GB but I would recommend 32GB).

Please do not buy or use gimmicky self-encrypting devices such as these:
https://syscall.eu/blog/2018/03/12/aigo_part1/ [Archive.org]

Some might be very efficient[259] but many are gimmicky gadgets that offer no real protection[260].

Find some safe places with decent public Wi-Fi:

You need to find safe places where you will be able to do your sensitive activities using some publicly accessible Wi-Fi (without any account/ID registration, avoid CCTVs).

This can be anywhere that will not be tied to you directly (your home/work) and where you can use the Wi-Fi for a while without being bothered. But also, a place where you can do this without being "noticed" by anyone.

If you think Starbucks is a good idea, you may reconsider:

- They probably have CCTVs in all their shops and keep those recordings for an unknown amount of time.
- You will need to buy a coffee to get the Wi-Fi access code in most. If you pay this coffee with an electronic method, they will be able to tie your Wi-Fi access with your identity.

Situational awareness is key and you should be constantly aware of your surroundings and avoid touristy places like it was plagued by Ebola. You want to avoid appearing on any picture/video of anyone while someone is taking a selfie, making a TikTok video or posting some travel picture on their Instagram. If you do, remember chances are high that those pictures will end up online (publicly or privately) with full metadata attached to them (time/date/geolocation) and your face. Remember these can and will be indexed by Facebook/Google/Yandex/Apple and probably all 3 letters agencies.

While this will not be available yet to your local police officers, it could be in the near future.

You will ideally need a set of 3-5 different places such as this to avoid using the same place twice. Several trips will be required over the weeks for the various steps in this guide.

You could also consider connect to these places from a safe distance for added security. See Appendix Q: Using long range Antenna to connect to Public Wi-Fis from a safe distance.

The Tails route:

This part of the guide will help you in setting up Tails if one of the following is true:

- You cannot afford a dedicated laptop
- Your dedicated laptop is just too old and too slow
- You have very low IT skills
- You decide to go with Tails anyway

Tails[261] stands for **The Amnesic Incognito Live System**. It is a bootable Live Operating System running from a USB key that is designed for leaving no traces and forcing all connections through the Tor network.

You pretty much insert the Tails USB key into your laptop, boot from it and you have a full operating system running with privacy and anonymity in mind. As soon as you shut down the computer, everything will be gone unless you saved it somewhere.

---

[259] NYTimes, Lost Passwords Lock Millionaires Out of Their Bitcoin Fortunes
https://www.nytimes.com/2021/01/12/technology/bitcoin-passwords-wallets-fortunes.html [Archive.org]

[260] Usenix.org, Shedding too much Light on a Microcontroller's Firmware Protection
https://www.usenix.org/system/files/conference/woot17/woot17-paper-obermaier.pdf [Archive.org]

[261] Wikipedia, Tails, https://en.wikipedia.org/wiki/Tails_(operating_system) [Wikiless] [Archive.org]

Tails is a very easy way to get going in no time with what you have and without much learning. It has extensive documentation and tutorials.

WARNING: Tails is not always up-to-date with their bundled software. And not always up-to-date with the Tor Browser updates either. You should always make sure you are using the latest version of Tails and you should use extreme caution when using bundled apps within Tails that might be vulnerable to exploits and reveal your location[262].

It does however have some drawbacks:

- Tails uses Tor and therefore you will be using Tor to access any resource on the internet. This alone will make you suspicious to most platforms where you want to create anonymous accounts (this will be explained in more details later).
- Your ISP (whether it is yours or some public Wi-Fi) will also see that you are using Tor and this could make you suspicious in itself.
- Tails does not include (natively) some of the software you might want to use later which will complicate things quite a bit if you want to run some specific things (Android Emulators for instance).
- Tails uses Tor Browser which while it is very secure will be detected as well by most platforms and will hinder you in creating anonymous identities on many platforms.
- Tails will not protect you more from the 5$ wrench[11].
- Tor in itself might not be enough to protect you from an adversary with enough resources as explained earlier.

Important Note: If your laptop is monitored/supervised and some local restrictions are in place, please read Appendix U: How to bypass (some) local restrictions on supervised computers**.**

You should also read Tails Documentation, Warnings, and limitations, before going further https://tails.boum.org/doc/about/warning/index.en.html [Archive.org]

Taking all this into account and the fact that their documentation is great, I will just redirect you towards their well-made and well-maintained tutorial:

https://tails.boum.org/install/index.en.html [Archive.org] , pick your flavor and proceed.

When you are done and have a working Tails on your laptop, go to the Creating your anonymous online identities step much further in this guide.

If you're having issue accessing Tor due to censorship or other issues, you can try using Tor Bridges by following this Tails tutorial: https://tails.boum.org/doc/first_steps/welcome_screen/bridge_mode/index.en.html [Archive.org] and find more information about these on Tor Documentation https://2019.www.torproject.org/docs/bridges [Archive org]

If you think using Tor alone is dangerous/suspicious, see Appendix P: Accessing the internet as safely as possible when Tor/VPN is not an option

Persistent Plausible Deniability using Whonix within Tails:

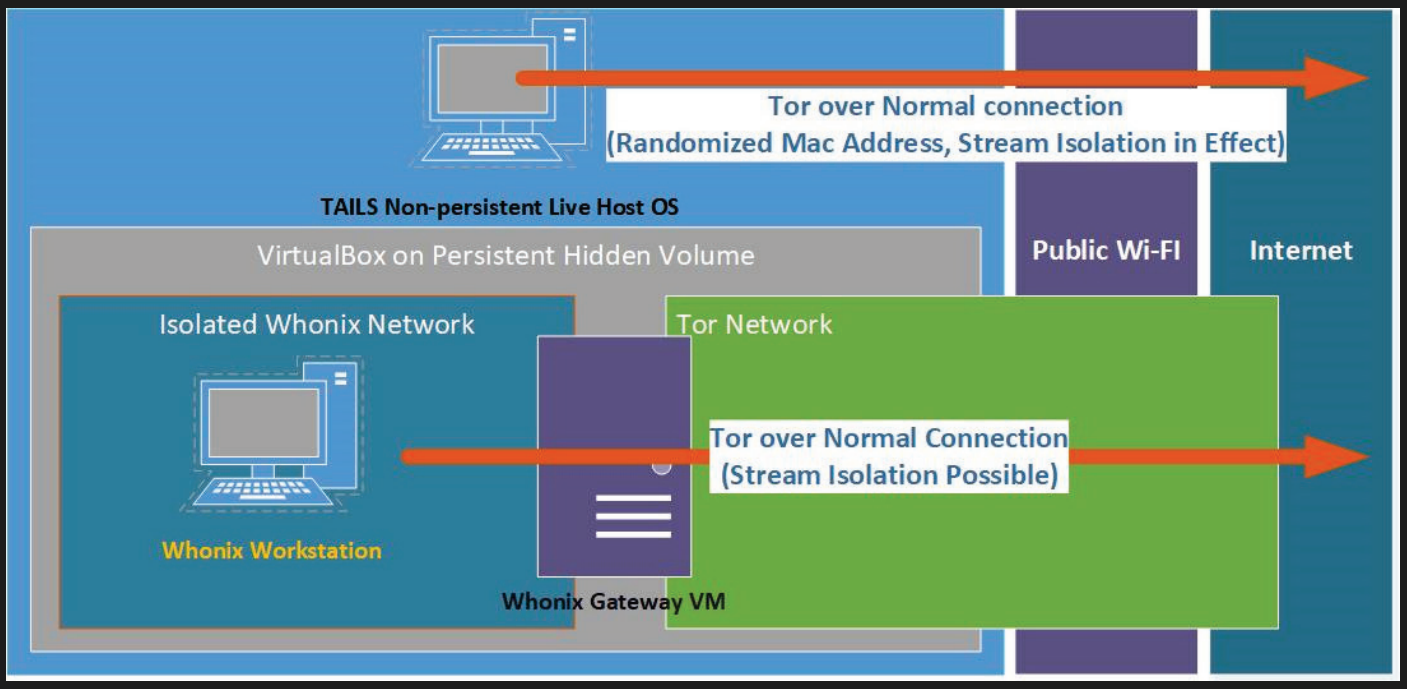
Consider checking the https://github.com/aforensics/HiddenVM [Archive.org] project for Tails.

This project is a clever idea of a one click self-contained VM solution that you could store on an encrypted disk using plausible deniability[272] (see The Whonix route: first chapters and also for some explanations about Plausible deniability, as well as the How to securely delete specific files/folders/data on your HDD/SSD and Thumb drives: section at the end of this guide for more understanding).

This would allow the creation of a hybrid system mixing Tails with the Virtualization options of the Whonix route in this guide.

---

[262] Vice.com, Facebook Helped the FBI Hack a Child Predator https://www.vice.com/en/article/v7gd9b/facebook-helped-fbi-hack-child-predator-buster-hernandez [Archive org]



Note: See Pick your connectivity method in the Whonix Route for more explanations about Stream Isolation

In short:

- You could run non-persistent Tails from one USB key (following their recommendations)
- You could store persistent VMs within a secondary contained that could be encrypted normally or using Veracrypt plausible deniability feature (these could be Whonix VMs for instance or any other).
- You do benefit from the added Tor Stream Isolation feature (see Tor over VPN for mor info about stream isolation).

In that case as the project outlines it, there should be no traces of any of your activities on your computer and the sensitive work could be done from VMs stored into a Hidden container that should not be easily discoverable by a soft adversary.

This option is particularly interesting for "traveling light" and to mitigate forensics attacks while keeping persistence on your work. You only need 2 USB keys (one with Tails and one with a Veracrypt container containing persistent Whonix). The first USB key will appear to contain just Tails and the second USB will appear to contain just random garbage but will have a decoy volume which you can show for plausible deniability.

You might also wonder if this will result in a "Tor over Tor" setup but it will not. The Whonix VMs will be accessing the network directly through clearnet and not through Tails Onion Routing.

In the future, this could also be supported by the Whonix project themselves as explained here: https://www.whonix.org/wiki/Whonix-Host [Archive.org] but it not yet recommended as of now for end-users.

Remember that encryption with or without plausible deniability is not a silver bullet and will be of little use in case of torture[11]. As a matter a fact, depending on who your adversary would be (your threat model), it might be wise not to use Veracrypt (formerly TrueCrypt) at all as shown in this demonstration: https://defuse.ca/truecrypt-plausible-deniability-useless-by-game-theory.htm [Archive org]

Plausible deniability is only effective against soft lawful adversaries that will not resort to physical means.

See https://en.wikipedia.org/wiki/Rubber-hose_cryptanalysis [Wikiless] [Archive.org]

CAUTION: Please see Appendix K: Considerations for using external SSD drives and Understanding HDD vs SSD sections if you consider storing such hidden VMs on an external SSD drive:

- **Do not use hidden volumes on SSD drives as this is not supported/recommended by Veracrypt[263].**
- **Use instead file containers instead of encrypted volumes.**
- **Make sure you do know how to clean data from an external SSD drive properly.**

Here is my guide on how to achieve this:

First Run:

- Download the latest HiddenVM release from https://github.com/aforensics/HiddenVM/releases [Archive.org]
- Download the latest Whonix XFCE release from https://www.whonix.org/wiki/VirtualBox/XFCE [Archive.org]
- Prepare a USB Key/Drive with Veracrypt
    - Create a Hidden Volume on the USB/Key Drive (I would recommend at least 16GB for the hidden volume)
    - In the Outer Volume, place some decoy files
    - In the Hidden Volume, place the HiddenVM appimage file
    - In the Hidden Volume, place the Whonix XFCE ova file
- Boot into Tails
- Setup the Keyboard layout as you want.
- Select Additional Settings and set an administrator (root) password (needed for installing HiddenVM)
- Start Tails
- Connect to a safe wi-fi (this is a required step for the rest to work)
- Go into Utilities and Unlock your Veracrypt (hidden) Volume (do not forget to check the hidden volume checkbox)
- Launch the HiddenVM appimage
- When prompted to select a folder, select the Root of the Hidden volume (where the Whonix OVA and HiddenVM app image files are).
- Let it do its thing (This will basically install Virtualbox within Tails with one click)
- When it is done, it should automatically start Virtualbox Manager.
- Import the Whonix OVA files (see Whonix Virtual Machines:)

Note, if during the import you are having issues such as "NS_ERROR_INVALID_ARG (0x80070057)", this is probably because there is not enough disk space on your Hidden volume for Whonix. Whonix themselves recommend 32GB of free space but that's probably not necessary and 10GB should be enough for a start. You can try working around this error by renaming the Whonix *.OVA file to *.TAR and decompressing it within Tails. When you are done with decompression, delete the OVA file and import the other files with the Import wizard. This time it might work.

Subsequent Runs:

- Boot into Tails
- Connect to Wi-Fi
- Unlock your Hidden Volume
- Launch the HiddenVM App
- This should automatically open VirtualBox manager and show your previous VMs from the first run

Steps for all other routes:

Get a dedicated laptop for your sensitive activities:

Ideally, you should get a dedicated laptop that will not be tied to you in any easy way (ideally paid with cash anonymously and using the same precautions as previously mentioned for the phone and the SIM card). It is recommended but not mandatory because this guide will help you harden your laptop as much as possible to prevent data leaks through various means. There will be several lines of defense standing between your online identities and yourself that should prevent most adversaries from de-anonymizing you besides state/global actors with considerable resources.

[263] Veracrypt Documentation, Trim Operations https://www.veracrypt.fr/en/Trim%20Operation.html [Archive.org]

This laptop should ideally be a clean freshly installed Laptop (Running Windows, Linux or MacOS), clean of your normal day to day activities and offline (never connected to the network yet). In the case of a Windows laptop, and if you used it before such a clean install, it should also not be activated (re-installed without a product key). Specifically in the case of MacBooks, it should never have been tied to your identity before in any means. So, buy second-hand with cash from an unknown stranger who does not know your identity

This is to mitigate some future issues in case of online leaks (including telemetry from your OS or Apps) that could compromise any unique identifiers of the laptop while using it (MAC Address, Bluetooth Address, and Product key …). But also, to avoid being tracked back if you need to dispose of the laptop.

If you used this laptop before for different purposes (like your day-to-day activities), all its hardware identifiers are probably known and registered by Microsoft or Apple. If later any of those identifiers is compromised (by malware, telemetry, exploits, human errors …) they could lead back to you.

The laptop should have at least 250GB of Disk Space **at least 6GB (ideally 8GB or 16GB)** of RAM and should be able to run a couple of Virtual Machines at the same time. It should have a working battery that lasts a few hours.

This laptop could have an HDD (7200rpm) or an SSD/NVMe drive. Both possibilities have their benefits and issues that will be detailed later.

All future online steps performed with this laptop should ideally be done from a safe network such as a Public Wi-Fi in a safe place (see Find some safe places with decent public Wi-Fi). But several steps will have to be taken offline first.

Some laptop recommendations:

If you can afford it, you might consider getting a Purism Librem laptop (https://puri.sm [Archive.org]) or System76 laptops (https://system76.com/ [Archive org]) while using Coreboot[264] (where Intel IME is disabled from factory).

In other cases, I would strongly recommend getting Business grade laptops (meaning not consumer/gaming grade laptops) if you can. For instance, some ThinkPad from Lenovo (my personal favorite). Here are lists of laptops currently supporting Libreboot and others where you can flash Coreboot yourself (that will allow you to disable Intel IME or AMD PSP):

- https://freundschafter.com/research/system-alternatives-without-intel-me-iamt-and-amd-psp-secure-technology/ [Archive.org]
- https://libreboot.org/docs/hardware/ [Archive.org]
- https://coreboot.org/status/board-status.html [Archive.org]

This is because those business laptops usually offer better and more customizable security features (especially in the BIOS/UEFI settings) with longer support than most consumer laptops (Asus, MSI, Gigabyte, Acer…). The interesting features to look for are IMHO:

- Better custom Secure Boot **settings (where you can selectively manage all the keys and not just use the Standard ones)**
- HDD/SSD passwords in addition to just BIOS/UEFI passwords.
- AMD laptops could be more interesting as some provide the ability to disable AMD PSP (the AMD equivalent of Intel IME) from the BIOS/UEFI settings by default. And, because AFAIK, AMD PSP was audited and contrary to IME was not found to have any "evil" functionalities[265]. However, if you are going for the Qubes OS Route consider Intel as they do not support AMD with their anti-evil-maid system[266].
- Secure Wipe tools from the BIOS (especially useful for SSD/NVMe drives, see Appendix M: BIOS/UEFI options to wipe disks in various Brands).

---

[264] Coreboot, https://www.coreboot.org/ [Archive.org]

[265] YouTube, 36C3 - Uncover, Understand, Own - Regaining Control Over Your AMD CPU https://www.youtube.com/watch?v=bKH5nGLgi08&t=2834s [Invidious]

[266] Qubes OS, Anti-Evil Maid, https://github.com/QubesOS/qubes-antievilmaid [Archive.org]

- Better control over the disabling/enabling of select peripherals (USB ports, Wi-Fis, Bluetooth, Camera, Microphone …).
- Better security features with Virtualization.
- Native anti-tampering protections.
- Longer support with BIOS/UEFI updates (and subsequent BIOS/UEFI security updates).
- Some are supported by Libreboot

Bios/UEFI/Firmware Settings of your laptop:

PC:

These settings can be accessed through the boot menu of your laptop. Here is a good tutorial from HP explaining all the ways to access the BIOS on various computers: https://store.hp.com/us/en/tech-takes/how-to-enter-bios-setup-windows-pcs [Archive.org]

Usually how to access it is pressing a specific key (F1, F2 or Del) at boot (before your OS).

Once you are in there, you will need to apply a few recommended settings:

- Disable Bluetooth completely if you can.
- Disable Biometrics (fingerprint scanners) if you have any if you can. However, you could add a biometric additional check for booting only (pre-boot) but not for accessing the BIOS/UEFI settings.
- Disable the Webcam and Microphone if you can.
- Enable BIOS/UEFI password and use a long passphrase instead of a password (if you can) and make sure this password is required for:
    - Accessing the BIOS/UEFI settings themselves
    - Changing the Boot order
    - Startup/Power-on of the device
- Enable HDD/SSD password if the feature is available. This feature will add another password on the HDD/SSD itself (not in the BIOS/UEFI firmware) that will prevent this HDD/SSD from being used in a different computer without the password. Note that this feature is also specific to some manufacturers and could require specific software to unlock this disk from a completely different computer.
- Prevent accessing the boot options (the boot order) without providing the BIOS/UEFI password if you can.
- Disable USB/HDMI or any other port (Ethernet, Firewire, SD card …) if you can.
- Disable Intel ME if you can.
- Disable AMD PSP if you can (AMD's equivalent to IME, see Your CPU)
- Disable Secure Boot if you intend to use QubesOS as they do not support it out of the box[267]. Keep it on if you intend to use Linux/Windows.
- Check if your laptop BIOS has a secure erase option for your HDD/SSD that could be convenient in case of need.

Only enable those on a "need to use" basis and disable then again after use. This can help mitigate some attacks in case your laptop is seized while locked but still on OR if you had to shut it down rather quickly and someone took possession of it (this topic will be explained later in this guide).

About Secure boot:

So, what is Secure Boot[268]? In short, it is a UEFI security feature designed to prevent your computer from booting an operating system from which the bootloader was not signed by specific keys stored in the UEFI firmware of your laptop.

[267] QubesOS FAQ, https://www.qubes-os.org/faq/#is-secure-boot-supported [Archive.org]

[268] Wikipedia, Secure Boot, https://en.wikipedia.org/wiki/Unified_Extensible_Firmware_Interface#Secure_boot [Wikiless] [Archive.org]

Basically, when the Operating Systems (or the Bootloader[269]) supports it, you can store the keys of your bootloader in your UEFI firmware and this will prevent booting up any unauthorized Operating System (such as a live OS USB or anything similar).

Secure Boot settings are protected be the password you setup to access the BIOS/UEFI settings. If you have that password, you can disable Secure Boot and allow unsigned OSes to boot on your system. This can help mitigate some Evil-Maid attacks (explained later in this guide).

In most cases Secure Boot is disabled by default or is enabled but in "setup" mode which will allow any system to boot. For Secure Boot to work, your Operating System will have support it and then sign its bootloader and push those signing keys to your UEFI firmware. After that you will have to go to your BIOS/UEFI settings and save those pushed keys from your OS and change the Secure Boot from setup to user mode (or custom mode in some cases).

After doing that step, only the Operating Systems from which your UEFI firmware can verify the integrity of the bootloader will be able to boot.

Most laptops will have some default keys already stored in the secure boot settings. Usually those from the manufacturer itself or from some companies such as Microsoft. So, this means that by default, it will always be possible to boot some USB disks even with secure boot. These includes Windows, Fedora, Ubuntu, Mint, Debian, CentOS, OpenSUSE, Tails, Clonezilla and many others. Secure Boot is however not supported at all by QubesOS at this point.

In some laptops, you can manage those keys and remove the ones you do not want with a "custom mode" to only authorize your own bootloader that you could sign yourself if you really want to.

So, what is Secure Boot protecting you from? It will protect your laptop from booting unsigned bootloaders (by the OS provider) with for instance injected malware.

What is Secure Boot not protecting you from?

- Secure Boot is not encrypting your disk and an adversary can still just remove the disk from your laptop and extract data from it using a different machine. Secure Boot is therefore useless without full disk encryption.
- Secure Boot is not protecting you from a signed bootloader that would be compromised and signed by the manufacturer itself (Microsoft for example in the case of Windows). Most mainstream Linux distributions are signed these days and will boot with Secure Boot enabled.
- Secure Boot can have flaws and exploits like any other system. If you are running an old laptop that does not benefit from new BIOS/UEFI updates, these can be left unfixed.

Additionally, there are number of attacks that could be possible against Secure Boot as explained (in depth) in these technical videos:

- Defcon 22, https://www.youtube.com/watch?v=QDSlWa9xQuA [Invidious]
- BlackHat 2016, https://www.youtube.com/watch?v=0fZdL3ufVOI [Invidious]

So, it can be useful as an added measure against some adversaries but not all. Secure Boot in itself is not encrypting your hard drive. It is an added layer but that is it.

I still recommend you keep it on if you can.

Mac:

Take a moment to set a firmware password according to the tutorial here: https://support.apple.com/en-au/HT204455 [Archive.org]

You should also enable firmware password reset protection (available from Catalina) according to the documentation here: https://support.apple.com/en-gb/guide/security/sec28382c9ca/web [Archive.org]

[269] Wikipedia, Booting https://en.wikipedia.org/wiki/Booting [Wikiless] [Archive.org]

This feature will mitigate the possibility for some adversaries to use hardware hacks to disable/bypass your firmware password. Note that this will also prevent Apple themselves from accessing the firmware in case of repair.

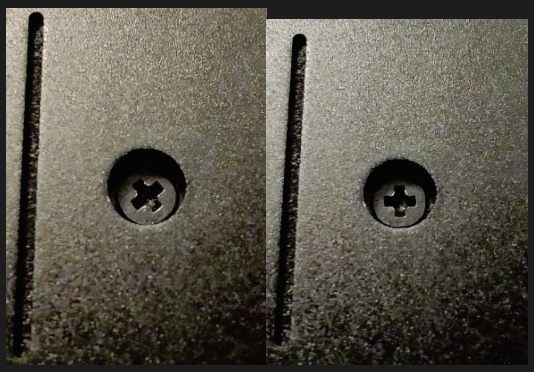
Physically Tamper protect your laptop:

At some point you will inevitably leave this laptop alone somewhere. You will not sleep with it and take it everywhere every single day. You should make it has hard as possible for anyone to tamper with it without you noticing it. This is mostly useful against some limited adversaries that will not use a 5$ wrench against you[11].

It is important to know that it is trivially easy for some specialists to install a key logger in your laptop, or to just make a clone copy of your hard drive that could later allow them to detect the presence of encrypted data in it using forensic techniques (more on that later).

Here is a good cheap method to make your laptop tamper proof using Nail Polish (with glitter) https://mullvad.net/en/help/how-tamper-protect-laptop/ [Archive.org] [270] (with pictures).

While this is a good cheap method, it could also raise suspicions as it is quite "noticeable" and might just reveal that you "have something to hide". So, there are more subtle ways of achieving the same result. You could also for instance make a close macro photography of the back screws of your laptop or just use a very small amount of candle wax within one of the screws that could just look like usual dirt. You could then check for tampering by comparing the photographs of the screws with new ones. Their orientation might have changed a bit if your adversary was not careful enough (Tightening them exactly the same way they were before). Or the wax within the bottom of a screw head might have been damaged compared to before.



Same techniques can be used with USB ports where you could just put a tiny amount of candle wax within the plug that would be damaged by inserting an USB key in it.

In riskier environments, check your laptop for tampering before using on a regular basis.

The Whonix route:

Picking your Host OS (the OS installed on your laptop):

This route will make extensive use of Virtual Machines[271], they will require a host OS to run the Virtualization software. You have 3 recommended choices in this part of the guide:

- Your Linux distribution of choice (excluding Qubes OS)
- Windows 10 (preferably Home edition due to the absence of Bitlocker)
- MacOS (Catalina or higher)

In addition, changes are high that your Mac is or has been tied to an Apple account (at the time or purchase or after signing-in) and therefore its unique hardware identifiers could lead back to you in case of hardware identifiers leak.

Linux is also not necessarily the best choice for anonymity depending on your threat model. This is because using Windows will allow us to conveniently use Plausible Deniability[272] (aka Deniable Encryption[273]) easily at the OS level.

---

[270] Wired https://www.wired.com/2013/12/better-data-security-nail-polish/ [Archive.org]

[271] Wikipedia, Virtual Machine https://en.wikipedia.org/wiki/Virtual_machine [Wikiless] [Archive.org]

[272] Wikipedia, Plausible Deniability https://en.wikipedia.org/wiki/Plausible_deniability [Wikiless] [Archive.org]

[273] Wikipedia, Deniable Encryption https://en.wikipedia.org/wiki/Deniable_encryption [Wikiless] [Archive.org]

Windows is also unfortunately at the same time a privacy nightmare[274] but is the only (convenient) option for using OS wide plausible deniability. Windows telemetry and telemetry blocking is also widely documented which should mitigate many issues.

So, what is Plausible Deniability? It is the ability for you to cooperate with an adversary requesting access to your device/data without revealing your true secret. All this using Deniable Encryption[275].

A soft lawful adversary could ask for your encrypted laptop password. At first you could refuse to give out any password (using your "right to remain silent", "right not to incriminate yourself") but some countries are implementing laws[276,277] to exempt this from such rights (because terrorists and "think of the children"). In that case you might have to reveal the password or maybe face jail time in contempt of court. This is where plausible deniability will come into play.

You could then reveal a password but that password will only give access to "plausible data" (a decoy OS). The forensics will be well aware that it is possible for you to have hidden data but should not be able to prove this **(if you do this right)**. You will have cooperated and the investigators will have access to something but not what you actually want to hide. Since the burden of proof should lie on their side, they will have no options but to believe you unless they have a proof that you have hidden data.

This feature can be used at the OS level (a plausible OS and a hidden OS) or at the files level where you will have an encrypted file container (similar to a zip file) where different files will be shown depending on the encryption password you use.

This also means you could set-up your own advanced "plausible deniability" setup using any Host OS by storing for instance Virtual Machines on a Veracrypt hidden volume container (be careful for traces in the Host OS tho that would need to be cleaned if the host OS is persistent, see Some additional measures against forensics section later). There is a project for achieving this within Tails (https://github.com/aforensics/HiddenVM [Archive.org]) which would make your Host OS non persistent and use plausible deniability within Tails.

In the case of Windows, plausible deniability is also the reason you should ideally have Windows 10 Home (and not Pro). This is because Windows 10 Pro natively offers a full-disk encryption system (Bitlocker[278]) where Windows 10 Home offers no full-disk encryption at all. We will later use a third-party open-source software for encryption that will allow full-disk encryption on Windows 10 Home. This will give you a good (plausible) excuse to use this software. While using this software on Windows 10 Pro would be suspicious.

Note about Linux: So, what about Linux and plausible deniability? Yes, it is kind of possible to achieve plausible deniability with Linux too[279]. But it is complicated to set-up and IMHO requires a skill level high enough that you probably do not need this guide to help you try it.

Unfortunately, encryption is not magic and there are some risks involved:

Threats with encryption:

The 5$ Wrench:

Remember that encryption with or without plausible deniability is not a silver bullet and will be of little use in case of torture[11]. As a matter a fact, depending on who your adversary would be (your threat model), it might be wise not to use Veracrypt (formerly TrueCrypt) at all as shown in this demonstration: https://defuse.ca/truecrypt-plausible-deniability-useless-by-game-theory.htm [Archive org]

---

[274] Privacytools.io, Don't use Windows 10 - It's a privacy nightmare https://privacytools.io/operating-systems/#win10 [Archive.org]

[275] Wikipedia, Deniable Encryption https://en.wikipedia.org/wiki/Deniable_encryption [Wikiless] [Archive.org]

[276] Wikipedia, Key Disclosure Laws https://en.wikipedia.org/wiki/Key_disclosure_law [Wikiless] [Archive.org]

[277] GP Digital, World map of encryption laws and policies https://www.gp-digital.org/world-map-of-encryption/ [Archive.org]

[278] Wikipedia, Bitlocker https://en.wikipedia.org/wiki/BitLocker [Wikiless] [Archive.org]

[279] Alpine Linux Wiki, Setting up a laptop https://wiki.alpinelinux.org/wiki/Setting_up_a_laptop [Archive.org]

Plausible deniability is only effective against soft lawful adversaries that will not resort to physical means. **Avoid, if possible, the use of plausible deniability capable software (such as Veracrypt) if your threat model includes hard adversaries. So, Windows users should in that case install Windows Pro as a Host OS and use Bitlocker instead.**

See https://en.wikipedia.org/wiki/Rubber-hose_cryptanalysis [Wikiless] [Archive.org]

Evil-Maid Attack:

Evil Maid Attacks[280] are conducted when someone tampers with your laptop while you are away. For install to clone your hard drive, install malware or a key logger. If they can clone your hard drive, they can compare one image of your hard drive at the time they took it while you were away with the hard drive when they seize it from you. If you used the laptop again in between, forensics examiners might be able to prove the existence of the hidden data by looking at the variations between the two images in what should be an empty/unused space. This could lead to strong evidence of the existence of a hidden data. If they install a key logger or malware within your laptop (software or hardware), they will be able to simply get the password from you for later use when they seize it. Such attacks can be done at your home, your hotel, a border crossing or anywhere you leave your devices unattended.

You can mitigate this attack by doing the following (as recommended earlier):

- Have a basic tamper protection (as explained previously) to prevent physical access to the internals of the laptop without your knowing. This will prevent them from cloning your disks and installing a physical key logger without your knowledge.
- Disable all the USB ports (as explained previously) within a password protected BIOS/UEFI. Again, they will not be able to turn them on (without physically accessing the motherboard to reset the BIOS) to boot a USB device that could clone your hard drive or install a software-based malware that could act as a key logger.
- Set-up BIOS/UEFI/Firmware passwords to prevent any unauthorized boot of an unauthorized device.
- Some OSes and Encryption software have anti-EvilMaid protection that can be enabled. This is the case with Windows/Veracrypt and QubeOS.

Cold-Boot Attack:

Cold Boot attacks[281] are trickier than the Evil Maid Attack but can be part of an Evil Maid attack as it requires an adversary to come into possession of your laptop while you are actively using your device or shortly afterward.

The idea is rather simple, as shown in this video[282], an adversary could theoretically quickly boot your device on a special USB key that would copy the content of the RAM (the memory) of the device after you shut it down. If the USB ports are disabled or if they feel like they need more time, they could open it and "cool down" the memory using a spray or other chemicals (liquid nitrogen for instance) preventing the memory decaying. They could then be able to copy its content for analysis. This memory dump could contain the key to decrypt your device. We will later apply a few principles to mitigate these.

In the case of Plausible Deniability, there have been some forensics studies[283] about technically proving the presence of the hidden data with a simple forensic examination (without a Cold Boot/Evil Maid Attack) but these have been contested by other studies[284] and by the maintainer of Veracrypt[285] so I would not worry too much about those yet.

The same measures used to mitigate Evil Maid attacks should be in place for Cold Boot attacks with some added ones:

---

[280] Wikipedia, Evil Maid Attack https://en.wikipedia.org/wiki/Evil_maid_attack [Wikiless] [Archive.org]

[281] Wikipedia, Cold Boot Attack https://en.wikipedia.org/wiki/Cold_boot_attack [Wikiless] [Archive org]

[282] CITP 2008 (https://www.youtube.com/watch?v=JDaicPIgn9U) [Invidious]

[283] ResearchGate, Defeating Plausible Deniability of VeraCrypt Hidden Operating Systems https://www.researchgate.net/publication/318155607_Defeating_Plausible_Deniability_of_VeraCrypt_Hidden_Operating_Systems [Archive org]

[284] SANS.org, Mission Implausible: Defeating Plausible Deniability with Digital Forensics https://www.sans.org/reading-room/whitepapers/forensics/mission-implausible-defeating-plausible-deniability-digital-forensics-39500 [Archive org]

[285] SourceForge, Veracrypt Forum https://sourceforge.net/p/veracrypt/discussion/technical/thread/53f33faf/ [Archive.org]

- If your OS or Encryption software allows it, you should consider encrypting the keys within RAM too (this is possible with Windows/Veracrypt and will be explained later)
- You should limit the use of Sleep stand-by and instead use Shutdown or Hibernate to prevent the encryption keys from staying in RAM when your computer goes to sleep. This is because sleep will maintain power to your memory for resuming your activity faster. Only hibernation and shutdown will actually clear the key from the memory[286].

See also https://www.whonix.org/wiki/Cold_Boot_Attack_Defense [Archive.org] and https://www.whonix.org/wiki/Protection_Against_Physical_Attacks [Archive.org]

Here are also some interesting tools to consider for Linux users to defend against these:

- https://github.com/0xPoly/Centry [Archive.org] (unfortunately unmaintained it seems so I made a fork and pull request updating for Veracrypt https://github.com/AnonymousPlanet/Centry [Archive.org] which should still work)
- https://github.com/hephaest0s/usbkill [Archive.org] (unfortunately unmaintained as well it seems)
- https://github.com/Lvl4Sword/Killer [Archive org]
- https://askubuntu.com/questions/153245/how-to-wipe-ram-on-shutdown-prevent-cold-boot-attacks [Archive org]
- (Qubes OS, Intel CPU only) https://github.com/QubesOS/qubes-antievilmaid [Archive.org]

About Sleep, Hibernation and Shutdown:

If you want the better security, you should shut down your laptop completely every time you leave it unattended or close the lid. This should clean and/or release the RAM and provide mitigations against cold boot attacks. However, this can be a bit inconvenient as you will have to reboot completely and type in a ton of passwords into various apps. Restart various VMs and other apps. So instead, you could also use hibernation instead (not supported on Qubes OS). Since the whole disk is encrypted, hibernation in itself should not pose a large security risk but will still shutdown your laptop and clear the memory while allowing you to conveniently resume your work afterward. **What you should never do it use the standard sleep feature which will keep your computer on and the memory powered. This is an attack vector against evil-maid and cold-boot attacks discussed earlier. This is because your powered on memory holds the encryption keys to your disk (encrypted or not) and could then be accessed by a skilled adversary.**

This guide will provide guidance later on how to enable hibernation on various host OSes (except Qubes OS) if you do not want to shut down every time.

Local Data Leaks (traces) and forensics examination:

As mentioned briefly earlier, these are data leaks and traces from your operating system and apps when you perform any activity on your computer. These mostly apply to encrypted file containers (with or without plausible deniability) than OS wide encryption. Such leaks are less "important" if your whole OS is encrypted (if you are not compelled to reveal the password).

Let us say for example you have a Veracrypt encrypted USB key with plausible deniability enabled. Depending on the password you use when mounting the USB key, it will open a decoy folder or the sensitive folder. Within those folders, you will have decoy documents/data within the decoy folder and sensitive documents/data within the sensitive folder.

In all cases, you will (most likely) open these folders with Windows Explorer, MacOS Finder or any other utility and do whatever you planned to do. Maybe you will edit a document within the sensitive folder. Maybe you will search a document within the folder. Maybe you will delete one or watch a sensitive video using VLC.

[286] Microsoft, BitLocker Countermeasures https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-countermeasures [Archive.org]

Well, all those Apps and your Operating System might keep logs and traces of that usage. This might include the full path of the folder/files/drives, the time those were accessed, temporary caches of those files, the "recent" lists in each apps, the file indexing system that could index the drive and even thumbnails that could be generated

Here are some examples of such leaks:

Windows:

- Windows ShellBags that are stored within the Windows Registry silently storing various histories of accessed volumes/files/folders[287].
- Windows Indexing keeping traces of the files present in your user folder by default[288].
- Recent lists (aka Jump Lists) in Windows and various apps keeping traces of recently accessed documents[289].
- Many more traces in various logs, please see this convenient interesting poster for more insight: https://www.sans.org/security-resources/posters/windows-forensic-analysis/170/download [Archive.org]

MacOS:

- Gatekeeper[290] and XProtect keeping track of your download history in a local database and file attributes.
- Spotlight Indexing
- Recent lists in various apps keeping traces of recently accessed documents.
- Temporary folders keeping various traces of App usage and Document usage.
- MacOS Logs
- …

Linux:

- Tracker Indexing
- Bash History
- USB logs
- Recent lists in various apps keeping traces of recently accessed documents.
- Linux Logs
- …

Forensics could[284,287] use all those leaks (see Local Data Leaks and Forensics) to prove the existence of hidden data and defeat your attempts at using plausible deniability and to find out about your various sensitive activities.

It will be therefore important to apply various steps to prevent forensics from doing this by preventing and cleaning these leaks/traces and more importantly by using whole disk encryption, virtualization, and compartmentalization.

Forensics cannot extract local data leaks from an OS they cannot access. And you will be able to clean most of those traces by wiping the drive or by securely erasing your virtual machines (which is not as easy as you think on SSD drives).

Some cleaning techniques will nevertheless be covered in the "Cover your Tracks" part of this guide at the very end.

Online Data Leaks:

Whether you are using simple encryption or plausible deniability encryption. Even if you covered your tracks on the computer itself. There is still a risk of online data leaks that could reveal the presence of hidden data.

---

[287] SANS, Windows ShellBag Forensics in-depth https://www.sans.org/reading-room/whitepapers/forensics/windows-shellbag-forensics-in-depth-34545 [Archive.org]

[288] University of York, Forensic data recovery from the Windows Search Database https://eprints.whiterose.ac.uk/75046/1/Forensic_Data_Recovery_From_The_Windows_Search_Database_preprint_DIIN328.pdf [Archive.org]

[289] A forensic insight into Windows 10 Jump Lists https://cyberforensicator.com/wp-content/uploads/2017/01/1-s2.0-S1742287616300202-main.2-14.pdf [Archive.org]

[290] Wikipedia, Gatekeeper https://en.wikipedia.org/wiki/Gatekeeper_(macOS) [Wikiless] [Archive.org]

Telemetry is your enemy. As explained earlier in this guide, the telemetry of Operating Systems but also from Apps can send staggering amounts of private information online.

In the case of Windows, this data could for instance be used to prove the existence of a hidden OS / Volume on a computer and would be readily available at Microsoft. Therefore, it is critically important that you disable and block telemetry with all the means at your disposal. No matter what OS you are using.

Conclusion:

You should never conduct sensitive activities from a non-encrypted system. And even if it is encrypted, you should probably never conduct sensitive activities from the Host OS itself. Instead, you should use a VM to be able to efficiently isolate and compartmentalize your activities and prevent local data leaks.

If you have little to no knowledge of Linux or if you want to use OS wide plausible deniability, I would recommend going for Windows (or back to the Tails route) for convenience. This guide will help you hardening it as much as possible to prevent leaks. This guide will also help you hardening MacOS and Linux as much as possible to prevent similar leaks.

If you have no interest for OS wide plausible deniability and want to learn to use Linux, I would strongly recommend going for Linux or the Qubes route if your hardware allows it.

In all cases, the host OS should never be used to conduct sensitive activities directly. The host OS will only be used to connect to a public Wi-Fi Access Point. It will be left unused while you conduct sensitive activities and should ideally not be used for any of your day-to-day activities.

Consider also reading **https://www.whonix.org/wiki/Full_Disk_Encryption#Encrypting_Whonix_VMs** [Archive.org]

Linux Host OS:

As mentioned earlier, I do not recommend using your daily laptop for very sensitive activities. Or at least I do not recommend using your in-place OS for these. Doing that might result in unwanted data leaks that could be used to de-anonymize you. If you have a dedicated laptop for this, you should reinstall a fresh clean OS. If you do not want to wipe your laptop and start over, you should consider the Tails route or proceed at your own risks.

I also recommend that you do the initial installation completely offline to avoid any data leak.

You should always remember that despite the reputation, Linux mainstream distributions (Ubuntu for instance) are not necessarily better at security than other systems such as MacOS and Windows. See this reference to understand why https://madaidans-insecurities.github.io/linux.html [Archive.org].

Full disk encryption:

There are two possibilities here with Ubuntu:

- (Recommended and easy) Encrypt as part of the installation process: https://ubuntu.com/tutorials/install-ubuntu-desktop [Archive.org]
    - This process requires the full erasure of your entire drive (clean install).
    - Just check the "Encrypt the new Ubuntu installation for security"
- (Tedious but possible) Encrypt after installation: https://help.ubuntu.com/community/ManualFullSystemEncryption [Archive.org]

For other distros, you will have to document yourself but it will likely be similar. Encryption during install is just much easier in the context of this guide.

Reject/Disable any telemetry:

- During the install, just make sure you do not allow any data collection if prompted.
- If you are not sure, just make sure you did not enable any telemetry and follow this tutorial if needed https://vitux.com/how-to-force-ubuntu-to-stop-collecting-your-data-from-your-pc/ [Archive.org]
- Any other distro: You will need to document yourself and find out yourself how to disable telemetry if there is any.

Disable anything unnecessary:

- Disable Bluetooth if enabled by following this guide https://www.addictivetips.com/ubuntu-linux-tips/disable-bluetooth-in-ubuntu/ [Archive.org] or issuing the following command:
  - ```sudo systemctl disable bluetooth.service --force```
- Disable Indexing if enabled by default (Ubuntu >19.04) by following this guide https://www.linuxuprising.com/2019/07/how-to-completely-disable-tracker.html [Archive.org] or issuing the following commands:
  - ```sudo systemctl --user mask tracker-store.service tracker-miner-fs.service tracker-miner-rss.service tracker-extract.service tracker-miner-apps.service tracker-writeback.service```
    - You can safely ignore any error if it says some service does not exist
  - ```sudo tracker reset -hard```

Hibernation:

As explained previously, you should not use the sleep features but shutdown or hibernate your laptop to mitigate some evil-maid and cold-boot attacks. Unfortunately, this feature is disabled by default on many Linux distros including Ubuntu. It is possible to enable it but it might not work as expected. Follow this information at your own risk. If you do not want to do this, you should never use the sleep function and power off instead (and probably set the lid closing behavior to power off instead of sleep).

Follow this tutorial to enable Hibernate: https://help.ubuntu.com/16.04/ubuntu-help/power-hibernate.html [Archive org]

After Hibernate is enabled, change the behavior so that your laptop will hibernate when you close the lid by following this tutorial for Ubuntu 20.04 http://ubuntuhandbook.org/index.php/2020/05/lid-close-behavior-ubuntu-20-04/ [Archive.org] and this tutorial for Ubuntu 18.04 https://tipsonubuntu.com/2018/04/28/change-lid-close-action-ubuntu-18-04-lts/ [Archive.org]

Unfortunately, this will not clean the key from memory directly from memory when hibernating. To avoid this at the cost of some performance, you might consider encrypting the swap file by following this tutorial: https://help.ubuntu.com/community/EnableHibernateWithEncryptedSwap [Archive.org]

These settings should mitigate cold boot attacks if you can hibernate fast enough.

Enable MAC address randomization:

- Ubuntu, follow these steps https://help.ubuntu.com/community/AnonymizingNetworkMACAddresses [Archive org].
- Any other distro: you will have to find the documentation yourself but it should be quite similar to the Ubuntu tutorial.
- Consider this tutorial which should still work: https://josh.works/shell-script-basics-change-mac-address [Archive org]

Hardening Linux:

As a light introduction for new Linux users, consider https://www.youtube.com/watch?v=Sa0KqbpLye4 [Invidious]

For more in-depth and advanced options, refer to:

- This excellent guide: https://madaidans-insecurities.github.io/guides/linux-hardening.html [Archive.org]
- This excellent wiki resource: https://wiki.archlinux.org/title/Security [Archive.org]
- These excellent scripts based on the guide and wiki above: https://codeberg.org/SalamanderSecurity/PARSEC [Archive.org]

Setting up a safe Browser:

See Appendix G: Safe Browser on the Host OS

MacOS Host OS:

Note: At this time, this guide will not support ARM M1 MacBooks (yet). Due to Virtualbox not supporting this architecture yet. It could however be possible if you use commercial tools like VMWare or Parallels but those are not covered in this guide.

As mentioned earlier, I do not recommend using your daily laptop for very sensitive activities. Or at least I do not recommend using your in-place OS for these. Doing that might result in unwanted data leaks that could be used to de-anonymize you. If you have a dedicated laptop for this, you should reinstall a fresh clean OS. If you do not want to wipe your laptop and start over, you should consider the Tails route or proceed at your own risks.

I also recommend that you do the initial installation completely offline to avoid any data leak.

Do not ever sign in with your Apple account using that Mac.

During the install:

- Stay Offline
- Disable all data sharing requests when prompted including location services
- Do not sign-in with Apple
- Do not enable Siri

Hardening MacOS:

As a light introduction for new MacOS users, consider https://www.youtube.com/watch?v=lFx5icuE6Io [Invidious]

Now to go more in-depth in securing and hardening your MacOS, I recommend reading this GitHub guide which should cover many of the issues: https://github.com/drduh/macOS-Security-and-Privacy-Guide [Archive.org]

Here are the basic steps you should take after your offline installation:

Enable Firmware password with "disable-reset-capability" option:

First you should set-up a firmware password following this guide from Apple: https://support.apple.com/en-us/HT204455 [Archive.org]

Unfortunately, some attacks are still possible and an adversary could disable this password so you should also follow this guide to prevent disabling the firmware password from anyone including Apple: https://support.apple.com/en-gb/guide/security/sec28382c9ca/web [Archive.org]

Enable Hibernation instead of sleep:

Again, this is to prevent some cold-boot and evil-maid attacks by powering down your RAM and cleaning the encryption key when you close the lid. You should always either hibernate or shutdown. On MacOS, the hibernate feature even has a special option to specifically clear the encryption key from memory when hibernating (while you might have to wait for the memory to decay on other Operating Systems). Once again there are no easy options to do this within the settings so instead, we will have to do this by running a few commands to enable hibernation:

- Open a Terminal
- Run: ```sudo pmset -a destroyfvkeyonstandby 1```
    - This command will instruct MacOS to destroy the Filevault key on Standby (sleep)
- Run: ```sudo pmset -a hibernatemode 25```
    - This command will instruct MacOS to power off the memory during sleep instead of doing a hybrid hibernate that keeps the memory powered on. It will result in slower wakes but will increase battery life.

Now when you close the lid of your MacBook, it should hibernate instead of sleep and mitigate attempts at performing cold-boot attacks.

In addition, you should also setup an automatic sleep (Settings > Energy) to that your MacBook will hibernate automatically if left unattended.

Disable unnecessary services:

Disable some unnecessary settings within the settings:

- Disable Bluetooth
- Disable the Camera and Microphone
- Disable Location Services
- Disable Airdrop
- Disable Indexing

Prevent Apple OCSP calls:

These are the infamous "unblockable telemetry" calls from MacOS Big Sur disclosed here: https://sneak.berlin/20201112/your-computer-isnt-yours/ [Archive.org]

You could block OCSP reporting by issuing the following command in Terminal:

- ``` sudo sh -c 'echo "127.0.0.1 ocsp.apple.com" >> /etc/hosts'```

But you should probably document yourself on the actual issue before acting. This page is a good place to start: https://blog.jacopo.io/en/post/apple-ocsp/ [Archive.org]

Up to you really. I would block it because I do not want any telemetry at all from my OS to the mothership without my specific consent. None.

Enable Full Disk encryption (Filevault):

You should enable full disk encryption on your Mac using Filevault according to this part of the guide: https://github.com/drduh/macOS-Security-and-Privacy-Guide#full-disk-encryption [Archive.org]

Be careful when enabling. Do not store the recovery key at Apple if prompted (should not be an issue since you should be offline at this stage). You do not want a third party to have your recovery key obviously.

MAC Address Randomization:

Unfortunately, MacOS does not offer a native convenient way of randomizing your MAC Address and so you will have to do this manually. This will be reset at each reboot and you will have to re-do it each time to ensure you do not use your actual MAC Address when connecting to various Wi-Fis

You can do by issuing the following commands in terminal (without the parentheses):

- (Turn the Wi-Fi off) ```networksetup -setairportpower en0 off```
- (Change the MAC Address) ```sudo ifconfig en0 ether 88:63:11:11:11:11```
- (Turn the Wi-Fi back on) ```networksetup -setairportpower en0 on```

Setting up a safe Browser:

See Appendix G: Safe Browser on the Host OS

Windows Host OS:

As mentioned earlier, I do not recommend using your daily laptop for very sensitive activities. Or at least I do not recommend using your in-place OS for these. Doing that might result in unwanted data leaks that could be used to de-anonymize you. If you have a dedicated laptop for this, you should reinstall a fresh clean OS. If you do not want to wipe your laptop and start over, you should consider the Tails route or proceed at your own risks.

I also recommend that you do the initial installation completely offline to avoid any data leak.

Installation:

You should follow Appendix A: Windows Installation

As a light introduction, consider watching https://www.youtube.com/watch?v=vNRics7tlqw [Invidious]

Enable MAC address randomization:

You should randomize your MAC address as explained earlier in this guide:

Go into Settings > Network & Internet > Wi-Fi > Enable Random hardware addresses

Alternatively, you could use this free piece of software: https://technitium.com/tmac/ [Archive.org]

Setting up a safe Browser:

See Appendix G: Safe Browser on the Host OS

Enable some additional privacy settings on your Host OS:

See Appendix B: Windows Additional Privacy Settings

Windows Host OS encryption:

If you intend to use system-wide plausible deniability:

Veracrypt[291] is the software I will recommend for full disk encryption, file encryption and plausible deniability. It is a fork of the well-known but deprecated and unmaintained TrueCrypt. It can be used for

- Full Disk simple encryption (your hard drive is encrypted with one passphrase).
- Full Disk encryption with plausible deniability (this means that depending on the passphrase entered at boot, you will either boot a decoy OS or a hidden OS).
- File container simple encryption (it is a large file that you will be able to mount within Veracrypt as if it was an external drive to store encrypted files within).
- File container with plausible deniability (it is the same large file but depending on the passphrase you use when mounting it, you will either mount a "hidden volume" or the "decoy volume").

It is to my knowledge the only (convenient and usable by anyone) free, open-source and openly audited[292] encryption software that also provides plausible deniability for general use and it works with Windows Home Edition.

Go ahead and download and install Veracrypt from: https://www.veracrypt.fr/en/Downloads.html [Archive.org]

After installation, please take a moment to review the following options that will help mitigate some attacks:

- Encrypt the memory with a Veracrypt option[293] (settings > performance/driver options > encrypt RAM) at a cost of 5-15% performance. This setting will also disable hibernation (which does not actively clear the key when hibernating) and instead encrypt the memory altogether to mitigate some cold-boot attacks.
- Enable the Veracrypt option to wipe the keys from memory if a new device is inserted (system > settings > security > clear keys from memory if a new device is inserted). This could help in case your system is seized while still on (but locked).
- Enable the Veracrypt option to mount volumes as removable volumes (Settings > Preferences > Mount volume as removable media). This will prevent Windows from writing some logs about your mounts in the Event logs[294] and prevent some local data leaks.
- Be careful and have a good situational awareness, if you sense something weird. Shut your laptop down as fast as possible.
- While Veracrypt newer versions do support Secure Boot, I would recommend disabling it from the BIOS as I prefer Veracrypt Anti-Evil Maid system over Secure Boot.

If you do not want to use encrypted memory (because performance might be an issue), you should at least enable hibernation instead of sleep. This will not clear the keys from memory (you are still vulnerable to cold boot attacks) but at least should mitigate them somewhat if your memory has enough time to decay.

More details later in Route A and B: Simple Encryption using Veracrypt (Windows tutorial).

---

[291] Wikipedia Veracrypt https://en.wikipedia.org/wiki/VeraCrypt [Wikiless] [Archive.org]

[292] OSTIF Veracrypt Audit, 2016, https://ostif.org/the-veracrypt-audit-results/ [Archive org]

[293] Veracrypt Documentation, Unencrypted Data in RAM https://www.veracrypt.fr/en/Unencrypted%20Data%20in%20RAM.html [Archive.org]

[294] Veracrypt Documentation, Data Leaks https://www.veracrypt.fr/code/VeraCrypt/plain/doc/html/Data%20Leaks.html [Archive org]

If you do not intend to use system-wide plausible deniability:

For this case, I will recommend the use of BitLocker instead of Veracrypt for the full disk encryption. The reasoning is that BitLocker does not offer a plausible deniability possibility contrary to Veracrypt. A hard adversary has then no incentive in pursuing his "enhanced" interrogation if you reveal the passphrase.

Normally, you should have installed Windows Pro in this case and BitLocker setup is quite straight-forward.

Basically you can follow the instructions here: https://support.microsoft.com/en-us/windows/turn-on-device-encryption-0c453637-bc88-5f74-5105-741561aae838 [Archive.org]

But here are the steps:

- Click the Windows Menu
- Type "Bitlocker"
- Click "Manage Bitlocker"
- Click "Turn On Bitlocker" on your System Drive
- Follow the instructions
    - **Do not save your recovery key to a Microsoft Account if prompted.**
    - **Only save the recovery key to an external encrypted drive. To bypass this, print the recovery key using the Microsoft Print to PDF printer and save the key within the Documents folder.**
    - **Encrypt Entire Drive (do not encrypt the used disk space only).**
    - **Use "New Encryption Mode"**
    - **Run the BitLocker Check**
    - **Reboot**
- Encryption should now ne started in the background (you can check by clicking the Bitlocker icon in the lower right side of the taskbar).

Enable Hibernation (optional):

Again, as explained earlier. You should never use the sleep feature to mitigate some cold-boot and evil-maid attacks. Instead, you should Shut down or hibernate. You should therefore switch your laptop for sleeping to hibernating when closing the lid or when your laptop goes to sleep.

(**Note that you cannot enable hibernation if you previously enabled RAM encryption within Veracrypt)**

The reason is that Hibernation will actually shutdown your laptop completely and clean the memory. Sleep on the other hand will leave the memory powered on (including your decryption key) and could leave your laptop vulnerable to cold-boot attacks.

By default, Windows 10 might not offer you this possibility so you should enable it by following this Microsoft tutorial: https://docs.microsoft.com/en-us/troubleshoot/windows-client/deployment/disable-and-re-enable-hibernation [Archive.org]

- Open an administrator command prompt (right click on Command Prompt and "Run as Administrator")
- Run: powercfg.exe /hibernate on
- Now run the additional command: ```**powercfg /h /type full**```
    - **This command will make sure your hibernate mode is full and will fully clean the memory (not securely tho).**

After that you should go into your power settings:

- Open the Control Panel
- Open System & Security
- Open Power Options
- Open "Choose what the power button does"
- Change everything from sleep to hibernate or shutdown
- Go back to the Power Options
- Select Change Plan Settings

- Select Advanced Power Settings
- Change all the Sleep Values for each Power Plan to 0 (Never)
- Make sure Hybrid Sleep is Off for each Power Plan
- Enable Hibernate After the time you would like
- Disable all the Wake timers

Deciding which sub-route you will take:

Now you will have to pick your next step between two options:

- Route A: Simple encryption of your current OS
  - Pros:
    - Does not require you to wipe your laptop
    - No issue with local data leaks
    - Works fine with an SSD drive
    - Works with any OS
    - Simple
  - Cons:
    - You could be compelled by adversary to reveal your password and all your secrets and will have no plausible deniability.
    - Danger of Online data leaks
- Route B: Simple encryption of your current OS with later use of plausible deniability on files themselves:
  - Pros:
    - Does not require you to wipe your laptop
    - Works fine with an SSD drive
    - Works with any OS
    - Plausible deniability possible with "soft" adversaries
  - Cons:
    - Danger of Online Data leaks
    - Danger of Local Data leaks (that will lead to more work to clean up those leaks)
- Route C: Plausible Deniability Encryption of your Operating system (you will have a "hidden OS" and a "decoy OS" running on the laptop):
  - Pros:
    - No issues with local Data leaks
    - Plausible deniability possible with "soft" adversaries
  - Cons:
    - Requires Windows (this feature is not "easily" supported on Linux).
    - Danger of online Data leaks
    - Requires full wipe of your laptop
    - No use with an SSD drive due to requirement of disabling Trim[295] Operations[296]. This will severely degrade the performance/health of your SSD drive over time.

As you can see, Route C only offers two privacy advantages over the others and it will only be of use against a soft lawful adversary. Remember https://en.wikipedia.org/wiki/Rubber-hose_cryptanalysis [Wikiless] [Archive.org].

Deciding which route you will take is up to you. Route A is a minimum.

Always be sure to check for new versions of Veracrypt frequently to ensure you benefit from the latest patches. Especially check this before applying large Windows updates that might break the Veracrypt bootloader and send you into a boot loop.

NOTE THAT BY DEFAULT VERACRYPT WILL ALWAYS PROPOSE A SYSTEM PASSWORD IN QWERTY (display the password as a test). This can cause issues if your boot input is using your laptop's keyboard (AZERTY for example)

---

[295] Wikipedia, Trim https://en.wikipedia.org/wiki/Trim_(computing) [Wikiless] [Archive.org]

[296] Veracrypt Documentation, Trim Operations https://www.veracrypt.fr/en/Trim%20Operation.html [Archive.org]

as you will have setup your password in QWERTY and will input it at boot time in AZERTY. So, make sure you check when doing the test boot what keyboard layout your BIOS is using. You could fail to log-in just because the QWERTY/AZERTY mix-up. If your BIOS boots using AZERTY, you will need to type the password in QWERTY within Veracrypt.

Route A and B: Simple Encryption using Veracrypt (Windows tutorial)

Skip this step if you used BitLocker instead earlier.

You do not have to have an HDD for this method and you do not need to disable Trim on this route. Trim leaks will only be of use to forensics in detecting the presence of a Hidden Volume but will not be of much use otherwise.

This route is rather straightforward and will just encrypt your current Operating System in place without losing any data. Be sure to read all the texts Veracrypt is showing you so you have a full understanding of what is going on.

- Launch VeraCrypt
- Go into Settings:
  - Settings > Performance/driver options > Encrypt RAM
  - System > Settings > Security > Clear keys from memory if a new device is inserted
  - System > Settings > Windows > Enable Secure Desktop
- Select System
- Select Encrypt System Partition/Drive
- Select Normal (Simple)
- Select Single-Boot
- Select AES as encryption Algorithm (click the test button if you want to compare the speeds)
- Select SHA-512 as hash Algorithm (because why not)
- Enter a strong passphrase (longer the better, remember Appendix A2: Guidelines for passwords and passphrases)
- Collect some entropy by randomly moving your cursor around until the bar is full
- Click Next as the Generated Keys screen
- To rescue disk[297] or not rescue disk, well that is up to you. I recommend making one (just in case), just make sure to store it outside your encrypted drive (USB key for instance, or wait and see the end of this guide for guidance on safe backups). This rescue disk will not store your passphrase and you will still need it to use it.
- Wipe mode:
  - If you have no sensitive data yet on this laptop, select None
  - If you have sensitive data on an SSD, Trim alone should take care of it[298] but I would recommend 1 pass (random data) just to be sure.
  - If you have sensitive data on an HDD, there is no Trim and I would recommend at least 1-pass.
- Test your setup. Veracrypt will now reboot your system to test the bootloader before encryption. This test must pass for encryption to go forward.
- After your computer rebooted and the test is passed. You will be prompted by Veracrypt to start the encryption process.
- Start the encryption and wait for it to complete.
- You are done, skip Route B and go the next steps.

There will be another section on creating encrypted file containers with Plausible Deniability on Windows.

Route B: Plausible Deniability Encryption with a Hidden OS (Windows only)

This is only supported on Windows.

This is only recommended on an HDD drive. This is not recommended on an SSD drive.

---

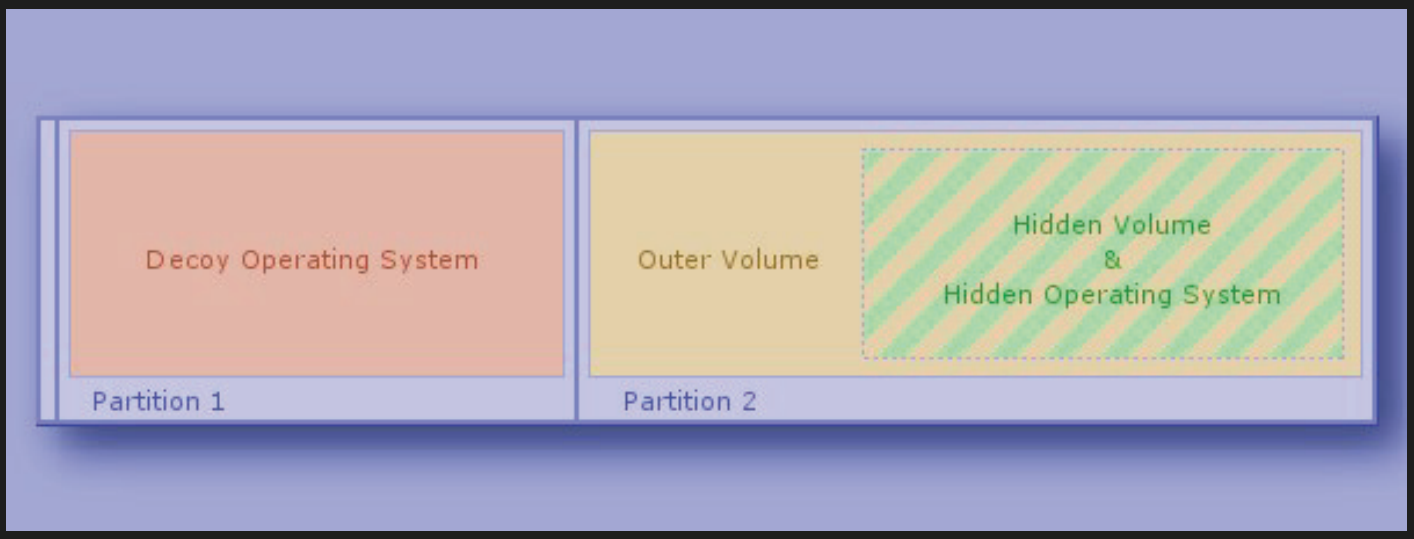
[297] Veracrypt Documentation, Rescue Disk https://www.veracrypt.fr/en/VeraCrypt%20Rescue%20Disk.html [Archive.org]

[298] St Cloud State University, Forensic Research on Solid State Drives using Trim Analysis https://repository.stcloudstate.edu/cgi/viewcontent.cgi?article=1141&context=msia_etds [Archive.org]

Your Hidden OS should not be activated (with a MS product key). Therefore, this route will recommend and guide you through a full clean installation that will wipe everything on your laptop.

Read the Veracrypt Documentation https://www.veracrypt.fr/en/VeraCrypt%20Hidden%20Operating%20System.html [Archive.org] (Process of Creation of Hidden Operating System part) and https://www.veracrypt.fr/en/Security%20Requirements%20for%20Hidden%20Volumes.html [Archive.org] (Security Requirements and Precautions Pertaining to Hidden Volumes).

This is how your system will look after this process is done:



(Illustration from Veracrypt Documentation, https://veracrypt.fr/en/VeraCrypt%20Hidden%20Operating%20System.html [Archive org])

As you can see this process requires you to have two partitions on your hard drive from the start.

This process will do the following:

- Encrypt your second partition (the outer volume) that will look like an empty unformatted disk from the decoy OS.
- Prompt you with the opportunity to copy some decoy content within the outer volume.
    - This is where you will copy your decoy Anime/Porn collection from some external hard drive to the outer volume.
- Create a hidden volume within the outer volume of that second partition. This is where the hidden OS will reside.
- Clone your currently running Windows 10 installation onto the hidden volume.
- Wipe your currently running Windows 10.
- This means that your current Windows 10 will become the hidden Windows 10 and that you will need to reinstall a fresh decoy Windows 10 OS.

Mandatory if you have an SSD drive and you still want to do this against the recommendation: Disable SSD Trim in Windows[299] (again this is NOT recommended at all as disabling Trim in itself is highly suspicious).Also as mentioned earlier, disabling Trim will reduce the lifetime of your SSD drive and will significantly impact its performance over time (your laptop will become slower and slower over several months of use until it becomes almost unusable, you will then have to clean the drive and re-install everything). But you must do it to prevent

[299] WindowsCentral, Trim Tutorial https://www.windowscentral.com/how-ensure-trim-enabled-windows-10-speed-ssd-performance [Archive.org]

data leaks[300] that could allow forensics to defeat your plausible deniability[301][302]. The only way around this at the moment is to have a laptop with a classic HDD drive instead.

Step 1: Create a Windows 10 install USB key

See Appendix C: Windows Installation Media Creation and go with the USB key route.

Step 2: Boot the USB key and start the Windows 10 install process (Hidden OS)

- Insert the USB key into your laptop
- See Appendix A: Windows Installation and proceed with installing Windows 10 Home.

Step 3: Privacy Settings (Hidden OS)

See Appendix B: Windows Additional Privacy Settings

Step 4: Veracrypt installation and encryption process start (Hidden OS)

Remember to read https://www.veracrypt.fr/en/VeraCrypt%20Hidden%20Operating%20System.html [Archive.org]

Do not connect this OS to your known Wi-Fi. You should download Veracrypt installer from a different computer and copy the installer here using an USB key.

- Install Veracrypt
- Start Veracrypt
- Go into Settings:
  - Settings > Performance/driver options > Encrypt RAM (**note that this option is not compatible with Hibernation your laptop and means you will have to shut down completely)**
  - System > Settings > Security > Clear keys from memory if a new device is inserted
  - System > Settings > Windows > Enable Secure Desktop
- Go into System and select Create Hidden Operating System
- Read all the prompts with thoroughly
- Select Single-Boot if prompted
- Create the Outer Volume using AES and SHA-512.
- Use all the space available on the second partition for the Outer Volume
- Use a strong passphrase (remember Appendix A2: Guidelines for passwords and passphrases)
- Select yes to Large Files
- Create some Entropy by moving the mouse around until the bar is full and select NTFS (do not select exFAT as we want this outer volume to look "normal" and NTFS is normal).
- Format the Outer Volume
- Open Outer Volume:
  - At this stage, you should copy decoy data onto the outer volume. So, you should have some sensitive but not so sensitive files/folders to copy there. In case you need to reveal a password to this Volume**.** This is a good place for your Anime/Mp3/Movies/Porn collection.
  - I recommend you do not fill the outer volume too much or too little (about 40%). Remember you must leave enough space for the Hidden OS (which will be same size as the first partition you created during installation).
- Use a strong passphrase for the Hidden Volume (obviously a different one than the one for the Outer Volume).
- Now you will create the Hidden Volume, select AES and SHA-512
- Fill the entropy bar until the end with random mouse movements
- Format the hidden Volume
- Proceed with the Cloning

---

[300] Veracrypt Documentation, Trim Operation https://veracrypt.eu/en/docs/trim-operation/ [Archive.org]

[301] Black Hat 2018, Perfectly Deniable Steganographic Disk Encryption https://i.blackhat.com/eu-18/Thu-Dec-6/eu-18-Schaub-Perfectly-Deniable-Steganographic-Disk-Encryption.pdf [Archive.org]

[302] Milan Broz's Blog, TRIM & dm-crypt ... problems? http://asalor.blogspot.com/2011/08/trim-dm-crypt-problems.html [Archive org]

- Veracrypt will now restart and Clone the Windows where you started this process into the Hidden Volume. This Windows will become your Hidden OS.
- When the cloning is complete, Veracrypt will restart within the Hidden System
- Veracrypt will inform you that the Hidden System is now installed and then prompt you to wipe the Original OS (the one you installed previously with the USB key).
- Use 1-Pass Wipe and proceed.
- Now your Hidden OS will be installed, proceed to next step

Step 5: Reboot and boot the USB key and start the Windows 10 install process again (Decoy OS)

Now that the Hidden OS is fully installed, you will need to install a Decoy OS.

- Insert the USB key into your laptop
- See Appendix A: Windows Installation and proceed with installing Windows 10 Home again (do not Install a different version and stick with Home).

Step 6: Privacy settings (Decoy OS)

See Appendix B: Windows Additional Privacy Settings

Step 7: Veracrypt installation and encryption process start (Decoy OS)

Now we will encrypt the Decoy OS:

- Install Veracrypt
- Launch VeraCrypt
- Select System
- Select Encrypt System Partition/Drive
- Select Normal (Simple)
- Select Single-Boot
- Select AES as encryption Algorithm (click the test button if you want to compare the speeds)
- Select SHA-512 as hash Algorithm (because why not)
- Enter a short weak password (yes this is serious, do it, it will be explained later).
- Collect some entropy by randomly moving your cursor around until the bar is full
- Click Next as the Generated Keys screen
- To rescue disk[303] or not rescue disk, well that is up to you. I recommend making one (just in case), just make sure to store it outside your encrypted drive (USB key for instance, or wait and see the end of this guide for guidance on safe backups). This rescue disk will not store your passphrase and you will still need it to use it.
- Wipe mode: Select 1-Pass just to be safe
- Pre-Test your setup. Veracrypt will now reboot your system to test the bootloader before encryption. This test must pass for encryption to go forward.
- After your computer rebooted and the test is passed. You will be prompted by Veracrypt to start the encryption process.
- Start the encryption and wait for it to complete.
- Your Decoy OS is now ready for use.

Step 8: Test your setup (Boot in Both)

Time to test your setup.

- Reboot and input your Hidden OS passphrase, you should boot within the Hidden OS.
- Reboot and input your Decoy OS passphrase, you should boot within the Decoy OS.
- Launch Veracrypt on the Decoy OS and mount the second partition using the Outer Volume Passphrase (mount it as read-only, by going into Mount Options and Selecting Read-Only) and it should mount the second partition as a read-only displaying your decoy data (your Anime/Porn collection). You are mounting it as read-only now because if you were to write data on it, you could override content from your Hidden OS.

[303] Veracrypt Documentation, Rescue Disk https://www.veracrypt.fr/en/VeraCrypt%20Rescue%20Disk.html [Archive.org]

Step 9: Changing the decoy data on your Outer Volume safely

Before going to next step, you should learn the way to mount your Outer Volume safely for writing content on it. This is also explained in this official Veracrypt Documentation
https://www.veracrypt.fr/en/Protection%20of%20Hidden%20Volumes.html [Archive.org]

You should do this from a safe trusted place.

Basically, you are going to mount your Outer Volume while also providing the Hidden Volume passphrase within the Mount Options to protect the Hidden Volume from being overwritten. Veracrypt will then allow you write data to the Outer volume without risking overwriting any data on the Hidden Volume.

This operation will not actually mount the Hidden Volume and should prevent the creation of any forensic evidence that could lead to the discovery of the Hidden OS. However, while you are performing this operation, both passwords will be stored in your RAM and therefore you could still be susceptible to a Cold-Boot Attack. To mitigate this, be sure to have the option to encrypt your RAM too.

- Open Veracrypt
- Select your Second Partition
- Click Mount
- Click Mount Options
- Check the "Protect the Hidden volume…" Option
- Enter the Hidden OS passphrase
- Click OK
- Enter your Outer Volume passphrase
- Click OK
- You should now be able to open and write to your Outer volume to change the content (copy/move/delete/edit…)

Step 10: Leave some forensics evidence of your outer Volume (with the decoy Data) within your Decoy OS

We must make the Decoy OS as plausible as possible. We also want your adversary to think you are not that smart.

Therefore, it is important to voluntarily leave some forensic evidence of your Decoy Content within your Decoy OS. This evidence will let forensic examiners see that you mounted your Outer Volume frequently to access its content.

Here are good tips to leave some forensics evidence:

- Play the content from the Outer Volume from your Decoy OS (using VLC for instance). Be sure to keep a history of those.
- Edit Documents and work in them.
- Enable File Indexing again on the Decoy OS and include the Mounted Outer Volume.
- Unmount it and mount it frequently to watch some Content.
- Copy some Content from your Outer Volume to your Decoy OS and then delete it unsafely (just put it in the recycle Bin).
- Have a Torrent Client installed on the Decoy OS use it from time to time to Download some similar stuff that you will leave on the Decoy OS.
- You could have a VPN client installed on the Decoy OS with a known VPN of yours (non-cash paid).

Do not put anything suspicious on the Decoy OS such as:

- This guide
- Any links to this guide
- Any suspicious anonymity software such as Tor Browser

Notes:

Remember that you will need valid excuses for this plausible deniability scenario to work:

Take some time to read again the "Possible Explanations for Existence of Two Veracrypt Partitions on Single Drive" of the Veracrypt documentation here https://www.veracrypt.fr/en/VeraCrypt%20Hidden%20Operating%20System.html [Archive.org]

- **You are using Veracrypt because you are using Windows 10 Home which does not feature Bitlocker but still wanted Privacy.**
- **You have two Partitions because you wanted to separate the System and the Data for easy organization and because some Geek friend told you this was better for performance.**
- **You have used a weak password for easy convenient booting on the System and a Strong long passphrase on the Outer Volume because you were too lazy to type a strong passphrase at each boot.**
- **You encrypted the second Partition with a different password than the System because you do not want anyone in your entourage to see your stuff. And so, you did not want that data available to anyone.**

Be careful:

- **You should never mount the Hidden Volume from the Decoy OS (NEVER EVER). If you did this, it will create forensics evidence of the Hidden Volume within the Decoy OS that could jeopardize your attempt at plausible deniability**. If you did this anyway (intentionally or by mistake) from the Decoy OS, there are ways to erase forensics evidence that will be explained later at the end of this guide.
- **Never ever Use the Decoy OS from the same network (public Wi-Fi) as the Hidden OS.**
- **When you do mount the Outer Volume from the Decoy OS, do not write any Data within the Outer Volume as this could override what looks like Empty Space but is in fact your Hidden OS. You should always mount it as read-only.**
- **If you want to change the Decoy content of the Outer Volume, you should use a Live OS USB Key that will run Veracrypt.**
- **Note that you will not use the Hidden OS to perform sensitive activities, this will be done later from a VM within the Hidden OS. The Hidden OS is only meant to protect you from a soft adversary that could gain access to your laptop and compel you to reveal your password.**
- **Be careful of any tampering with your laptop. Evil-Maid Attacks can reveal your hidden OS.**

Virtualbox on your Host OS:

Remember Appendix W: Virtualization.

This step and the following steps should be done from within the Host OS. This can either be your Host OS with simple encryption (Windows/Linux/MacOS) or your Hidden OS with plausible deniability (Windows only).

In this route, we will make extensive use of the free Oracle Virtualbox[304] software. This is a virtualization software in which you can create Virtual Machines that emulate a computer running a specific OS (if you want to use something else like Xen, Qemu, KVM or VMWARE, feel free to do so but this part of the guide covers Virtualbox only for convenience).

So, you should be aware that Virtualbox is not the virtualization software with the best track record in terms of security and some of the reported issues[305] have not be completely fixed to this date[306] and if you are using Linux with a bit more technical skills, you should consider using KVM instead by following the guide available at Whonix here https://www.whonix.org/wiki/KVM [Archive.org] and here https://www.whonix.org/wiki/KVM#Why_Use_KVM_Over_VirtualBox.3F [Archive.org]

Some steps should be taken in all cases:

All your sensitive activities will be done from within a guest Virtual Machine running Windows 10 Pro (not Home this time), Linux or MacOS.

---

[304] Wikipedia, Virtualbox https://en.wikipedia.org/wiki/VirtualBox [Wikiless] [Archive.org]

[305] VirtualBox Ticket 17987 https://www.virtualbox.org/ticket/17987 [Archive.org]

[306] Whonix Documentation, Spectre Meltdown, https://www.whonix.org/wiki/Spectre_Meltdown#VirtualBox [Archive.org]

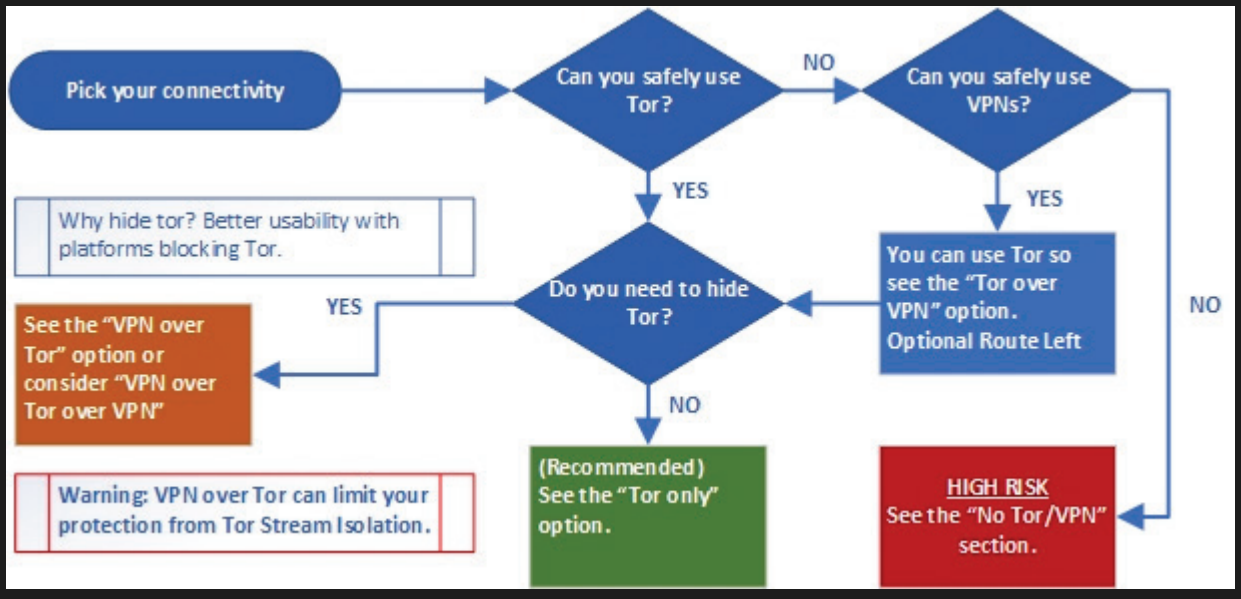
This has a few advantages that will greatly help you remain anonymous:

- It should prevent the guest VM OS (Windows/Linux/MacOS), Apps and any telemetry within the VMs from accessing your hardware directly. Even if your VM is compromised by malware, this malware should not be able to the VM and compromise your actual laptop.
- It will allow us to force all the network traffic from your client VM to run through another Gateway VM that will direct (torify) all the traffic towards the Tor Network. This is a network "kill switch". Your VM will lose its network connectivity completely and go offline if the other VM loses its connection to the Tor Network.
- The VM itself that only has internet connectivity through a Tor Network Gateway will connect to your cash-paid VPN service through Tor.
- DNS Leaks will be impossible because the VM is on an isolated network that must go through Tor no matter what.

Pick your connectivity method:

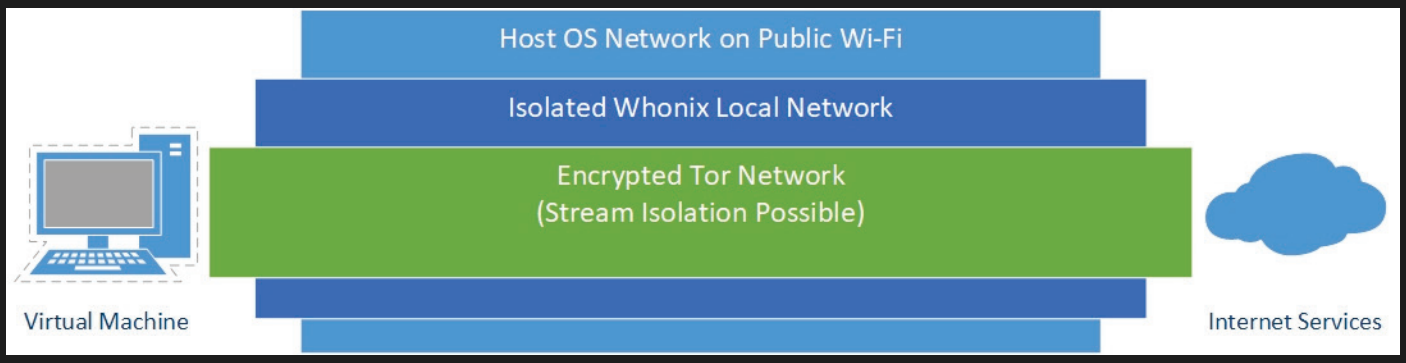
There are 7 possibilities within this route:

- **Recommended and preferred:**
  - **Use Tor alone (User > Tor > Internet)**
  - **Use VPN over Tor (User > Tor > VPN > Internet) in specific cases**
- Possible if required by context:
  - Use VPN over Tor over VPN (User > VPN > Tor > VPN > Internet)
  - Use Tor over VPN (User > VPN > Tor > Internet)
- Not recommended and risky:
  - Use VPN alone (User > VPN > Internet)
  - Use VPN over VPN (User > VPN > VPN > Internet)
- **Not recommended and highly risky (but possible)**
  - No VPN and no Tor (User > Internet)



Tor only:

This is the preferred and most recommended solution.



With this solution, all your network goes through Tor and it should be sufficient to guarantee your anonymity in most cases.

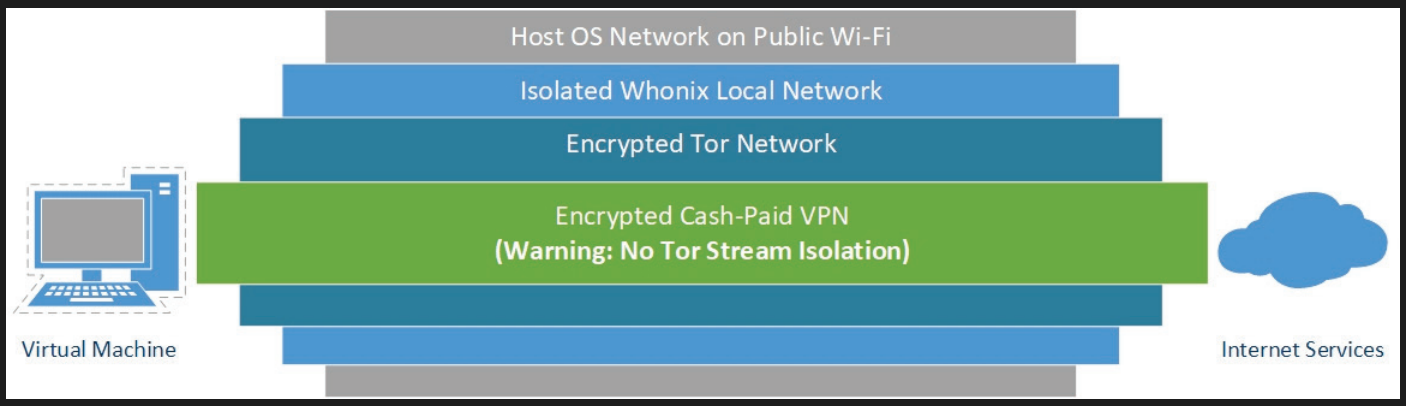
There is one main drawback tho: **Some services block/ban Tor Exit nodes outright and will not allow account creations from those.**

To mitigate this, you might have to consider the next option: VPN over Tor but consider some risks associated with it explained in the next section.

VPN/Proxy over Tor:

This solution can bring some benefits in some specific cases vs using Tor only where accessing the destination service would be impossible from a Tor Exit node. This is because many services will just outright ban, hinder, or block Tor (see https://gitlab.torproject.org/legacy/trac/-/wikis/org/doc/ListOfServicesBlockingTor [Archive.org]).

As you can see in this illustration, if your cash (preferred)/Monero paid VPN/Proxy is compromised by an adversary (despite their privacy statement and no-logging policies), they will only find an anonymous cash/Monero paid VPN/Proxy account connecting to their services from a Tor Exit node.



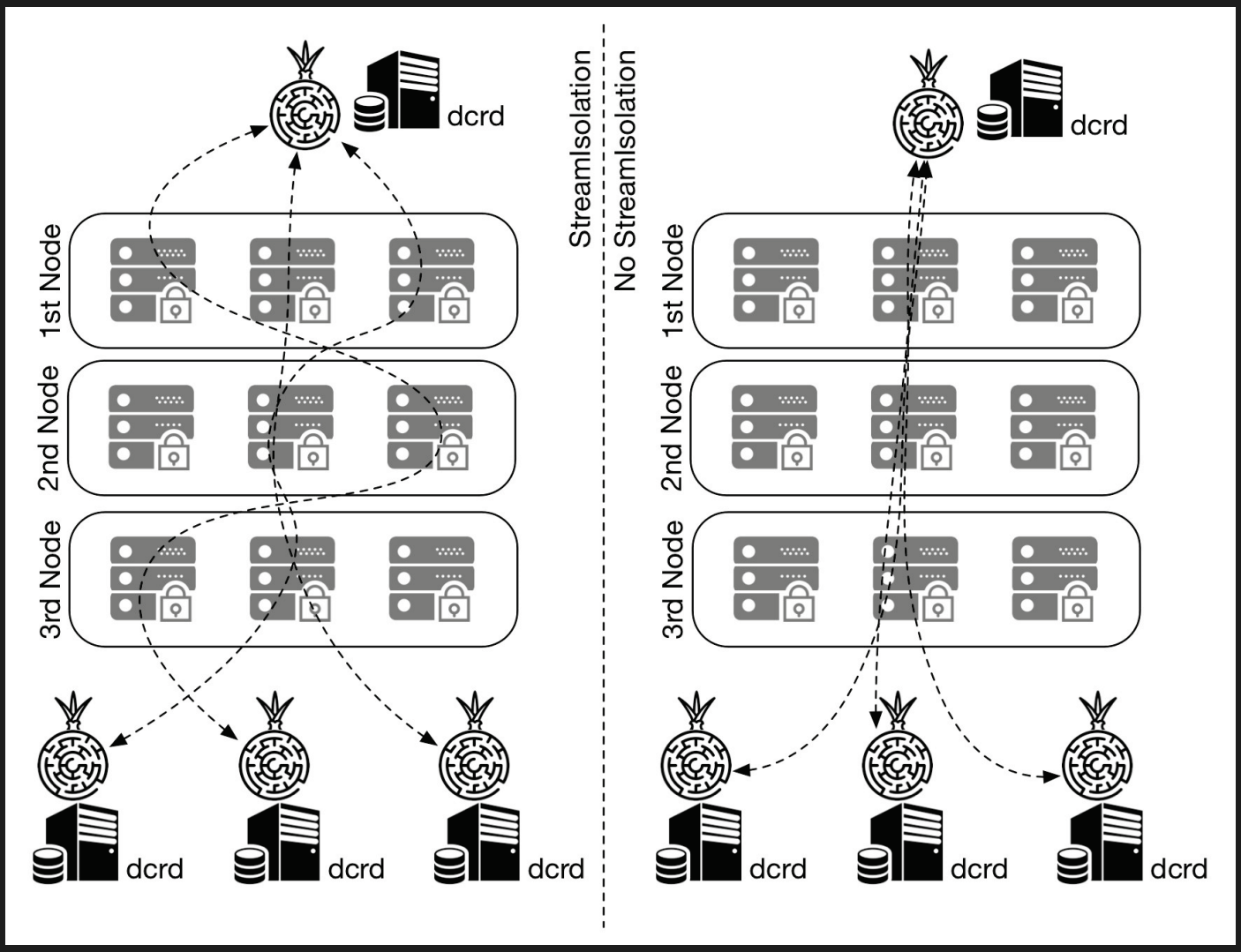
If an adversary somehow manages to compromise the Tor network too, they will only reveal the IP of a random public Wi-Fi that is not tied to your identity.

If an adversary somehow compromises your VM OS (with a malware or exploit for instance), they will be trapped within the internal Network of Whonix and should be unable to reveal the IP of the public Wi-Fi.

This solution however has one main drawback to consider: Interference with Tor Stream Isolation[307].

Stream isolation is a mitigation technique used to prevent some correlation attacks by having different Tor Circuits for each application. Here is an illustration to show what stream isolation is:

[307] Whonix Documentation, Stream Isolation https://www.whonix.org/wiki/Stream_Isolation [Archive.org]



(Illustration from Marcelo Martins, https://stakey.club/en/decred-via-tor-network/ [Archive.org])

VPN/Proxy over Tor falls on the right-side[308] meaning using a VPN/Proxy over Tor forces Tor to use one circuit for all activities instead of multiple circuits for each. This means that using a VPN/Proxy over Tor can somewhat reduce the effectiveness of Tor in some cases and should therefore be used only for some specific cases:

- When your destination service does not allow Tor Exit nodes.
- When you do not mind using a shared Tor circuit for various services. Like for instance for using various authenticated services.

You should however consider not using this method when your aim is just to browse random various unauthenticated websites as you will not benefit from Stream Isolation and this could make correlation attacks easier over time for an adversary between each of your sessions (see Your Anonymized Tor/VPN traffic). If your goal however is to use the same identity at each session on the same authenticated services, the value of Stream isolation is lessened as you can be correlated through other means.

You should also know that Stream Isolation is not necessarily configured by default on Whonix Workstation. It is only pre-configured for some applications (including Tor Browser).

Also note that Stream Isolation does not necessarily change all the nodes in your Tor circuit. It can sometimes only change one or two. In many cases, Stream Isolation (for instance within the Tor Browser) will only change the relay (middle) node and the exit node while keeping the same guard (entry) node.

More information at:

[308] Whonix Documentation, Tunnels Comparison Table, https://www.whonix.org/wiki/Tunnels/Introduction#Comparison_Table [Archive org]

- https://www.whonix.org/wiki/Stream_Isolation [Archive org]
- https://tails.boum.org/contribute/design/stream_isolation/ [Archive org]
- https://www.whonix.org/wiki/Tunnels/Introduction#Comparison_Table [Archive.org]

Tor over VPN:
You might be wondering: Well, what about using Tor over VPN instead of VPN over Tor? Well, I would not necessarily it:

- Disadvantages
  - Your VPN provider is just another ISP that will then know your origin IP and will be able to de-anonymize you if required. We do not trust them. I prefer a situation where your VPN provider does not know who you are. It does not add much in terms of anonymity.
  - This would result in you connecting to various services using the IP of a Tor Exit Node which are banned/flagged in many places. It does not help in terms of convenience.
- Advantages:
  - **The main advantage really is that if you are in a hostile environment where Tor access is impossible/dangerous/suspicious but VPN is okay.**
  - This method also does not break Tor Stream isolation.

Note, if you are having issues accessing the Tor Network due to blocking/censorship, you could try using Tor Bridges. See Appendix X: Using Tor bridges in hostile environments.

It is also possible to consider **VPN over Tor over VPN (User > VPN > Tor > VPN > Internet)** using two cash/Monero paid VPNs instead. This means that you will connect the Host OS to a first VPN from your Public Wi-Fi, then Whonix will connect to Tor and finally your VM will connect to a second VPN over Tor over VPN (see https://www.whonix.org/wiki/Tunnels/Connecting_to_a_VPN_before_Tor [Archive.org]).

This will of course have a significant performance impact and might be quite slow but I think Tor is necessary somewhere for achieving reasonable anonymity.

Achieving this technically is easy within this route, you need two separate anonymous VPN accounts and must connect to the first VPN from the Host OS and follow the route.

Conclusion: Only do this if you think using Tor alone is risky/impossible but VPNs are okay. Or just because you can and so why not.

VPN only:
This route will not be explained nor recommended.

If you can use VPNs then you should be able to add a Tor layer over it. And if you can use Tor, then you can add an anonymous VPN over Tor to get the preferred solution.

Just using a VPN or even a VPN over VPN makes no sense as those can be traced back to you over time. One of the VPN providers will know your real origin IP (even if it is in a safe public space) and even if you add one over it, the second one will still know you were using that other first VPN service. This will only slightly delay your de-anonymization. Yes, it is an added layer … but it is a persistent centralized added layer and you can be de-anonymized over time. This is just chaining 3 ISPs that are all subject to lawful requests.

For more info, please see the following references:

- https://www.whonix.org/wiki/Comparison_Of_Tor_with_CGI_Proxies,_Proxy_Chains,_and_VPN_Services#Tor_and_VPN_Services_Comparison [Archive.org]
- https://www.whonix.org/wiki/Why_does_Whonix_use_Tor [Archive.org]
- https://www.researchgate.net/publication/324251041_Anonymity_communication_VPN_and_Tor_a_comparative_study [Archive.org]
- https://gist.github.com/joepie91/5a9909939e6ce7d09e29#file-vpn-md [Archive org]
- https://schub.wtf/blog/2019/04/08/very-precarious-narrative.html [Archive.org]

In the context of this guide, Tor is required somewhere to achieve reasonable and safe anonymity and you should use it if you can.

No VPN/Tor:

If you cannot use VPN nor Tor where you are, you probably are in a very hostile environment where surveillance and control is very high.

Just do not, it is not worth it and too risky IMHO. You can be de-anonymized almost instantly by any motivated adversary that could get to your physical location in a matter of minutes.

Do not forget to check back on Adversaries (threats) and Appendix S: Check your network for surveillance/censorship using OONI.

If you have absolutely no other option and still want to do something, see Appendix P: Accessing the internet as safely as possible when Tor/VPN is not an option **(at your own risk) and consider The Tails route instead.**

Conclusion:

Connection Type	Anonymity	Ease of Access to online resources	Tor Stream isolation	Safer where Tor is suspicious/ dangerous	Speed	Cost	Recommended
Tor Alone	Good	Medium	Possible	No	Medium	Free	Yes
Tor over VPN	Good+	Medium	Possible	Yes	Medium	Around 50€/y	If needed (Tor inaccessible)
Tor over VPN over Tor	Best	Medium	Possible	Yes	Poor	Around 50€/y	Yes
VPN/Proxy over Tor	Good-	Good	No	No	Medium	Around 50€/y	If needed (convenience)
VPN/Proxy over Tor over VPN	Good-	Good	No	Yes	Poor	Around 100€/y	If needed (convenience and Tor inaccessible)
VPN/Proxy Alone	Bad	Good	N/A	Yes	Good	Around 50€/y	No, this is just non-sense.
No Tor and VPN	Bad	Unknown	N/A	No	Good	Around 100€ (Antenna)	No. At your own risk.

Unfortunately, using Tor alone will raise the suspicion of many destinations' platforms. You will face many hurdles (captchas, errors, difficulties signing-up) if you only use Tor. In addition, using Tor where you are could put you in trouble just for that. But Tor remains the best solution for anonymity and must be somewhere for anonymity.

- If your intent is to create persistent shared and authenticated identities on various services where access from Tor is hard, I recommend the **VPN over Tor** option (or VPN over Tor over VPN if needed). It might be a little less secure against correlation attacks due to breaking Tor Stream isolation but provides much better convenience in accessing online resources than just using Tor. It is an "acceptable" trade-off IMHP if you are careful enough with your identity.
- If your intent however is just to browse random services anonymously without creating specific shared identities, using tor friendly services; or if you do not want to accept that trade-off in the previous option. **Then I recommend using the Tor Only route to keep the full benefits of Stream Isolation (or Tor over VPN if you need to).**
- If cost is an issue, I recommend the Tor Only option if possible.
- If both Tor and VPN access are impossible or dangerous then you have no choice but to rely on Public wi-fis safely. See Appendix P: Accessing the internet as safely as possible when Tor and VPNs are not an option

For more information, you can also see the discussions here that could help decide yourself:

- Tor Project: https://gitlab.torproject.org/legacy/trac/-/wikis/doc/TorPlusVPN [Archive.org]

- Tails Documentation:
  - https://gitlab.tails.boum.org/tails/blueprints/-/wikis/vpn_support/ [Archive.org]
  - https://tails.boum.org/support/faq/index.en.html#index20h2 [Archive.org]
- Whonix Documentation (in this order):
  - https://www.whonix.org/wiki/Tunnels/Introduction [Archive.org]
  - https://www.whonix.org/wiki/Tunnels/Connecting_to_Tor_before_a_VPN [Archive.org]
  - https://www.whonix.org/wiki/Tunnels/Connecting_to_a_VPN_before_Tor [Archive.org]
- Some papers on the matter:
  - https://www.researchgate.net/publication/324251041_Anonymity_communication_VPN_and_Tor_a_comparative_study [Archive.org]

Get an anonymous VPN/Proxy:

Skip this step if you want to use Tor only.

See Appendix O: Get an anonymous VPN/Proxy

Whonix:

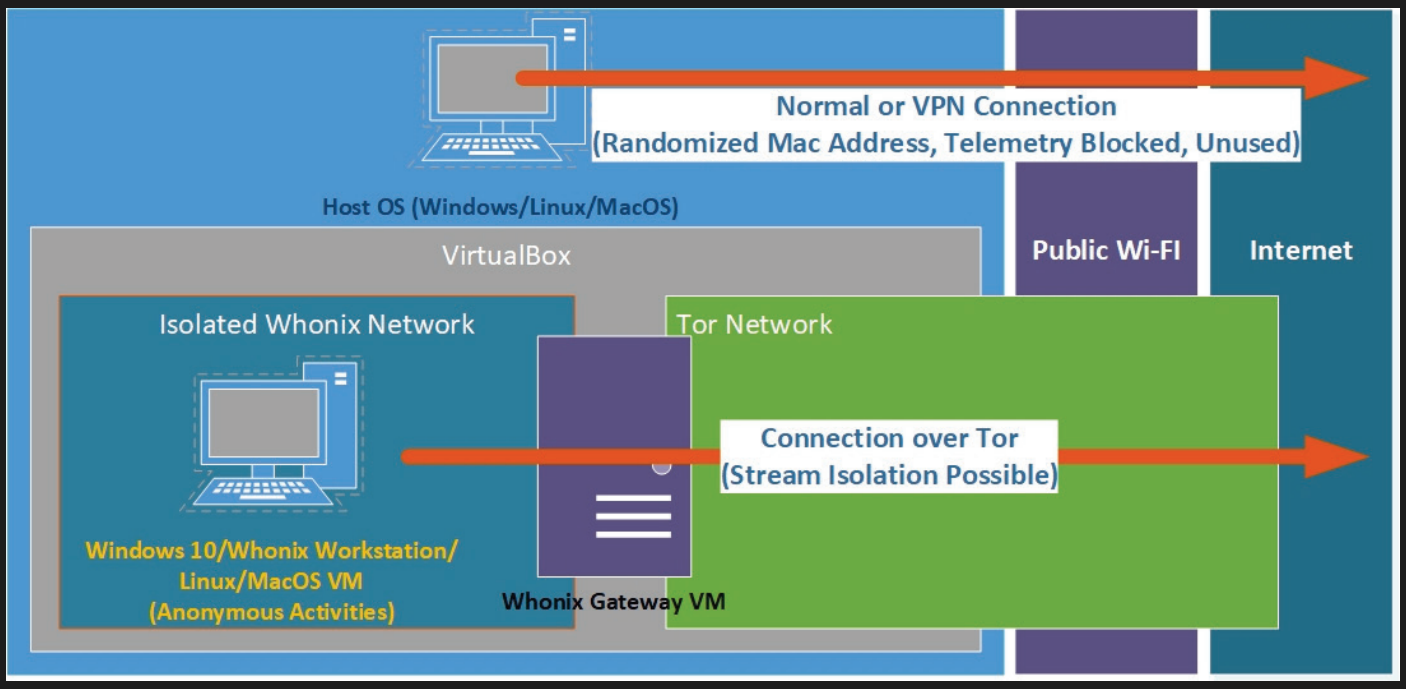
Skip this step if you cannot use Tor.

This route will use Virtualization and Whonix[309] as part of the anonymization process. Whonix is a Linux distribution composed of two Virtual Machines:

- The Whonix Workstation (this is a VM where you can conduct sensitive activities)
- The Whonix Gateway (this VM will establish a connection to the Tor network and route all the network traffic from the Workstation through the Tor network).

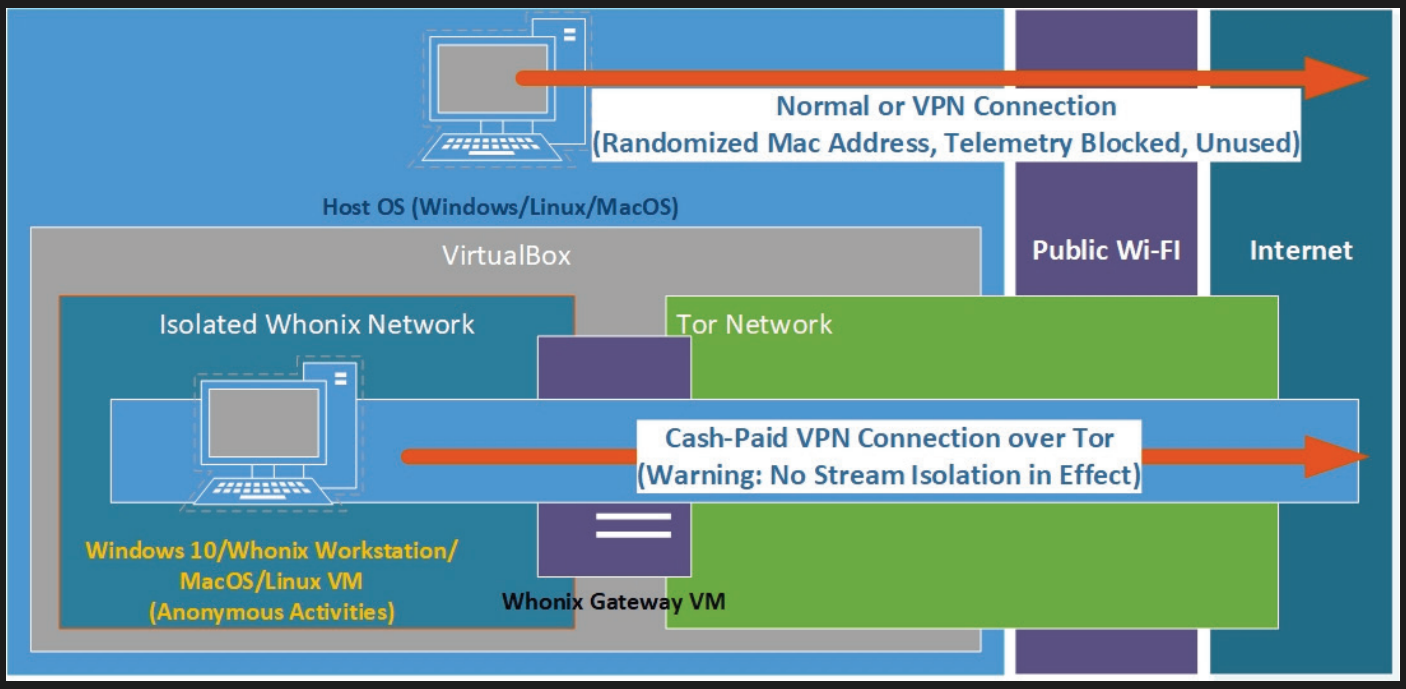
This guide will therefore propose 2 flavors of this route:

- The Whonix only route where all traffic is routed through the Tor Network (Tor Only or Tor over VPN).



- A Whonix hybrid route where all traffic is routed through a cash (preferred)/Monero paid VPN over the Tor Network (VPN over Tor or VPN over Tor over VPN).

[309] Wikipedia, Whonix https://en.wikipedia.org/wiki/Whonix [Wikiless] [Archive.org]



You will be able to decide which flavor to use based on my recommendations. I recommend the second one as explained before.

Whonix is well maintained and has extensive and incredibly detailed documentation.

A note on Virtualbox Snapshots:

Later, you will create and run several Virtual Machines within Virtualbox for your sensitive activities. Virtualbox provides a feature called "Snapshots"[310] that allow for saving the state of a VM at any point in time. If for any reason later you want to go back to that state, you can restore that snapshot at any moment.

I strongly recommend that you do make use of this feature by creating a snapshot after the initial installation / update of each VM. This snapshot should be done before their use for any sensitive/anonymous activity.

This will allow you to turn your VMs into a kind of a disposable "Live Operating Systems" (like Tails discussed earlier). Meaning that you will be able to erase all the traces of your activities within a VM by restoring a Snapshot to an earlier state. Of course, this will not be "as good" as Tails (where everything is stored in memory) as there might be traces of this activity left on your hard disk. Forensics studies have shown the ability to recover data from a reverted VM[311]. Fortunately, there will be ways to remove those traces after deletion or reverting to a previous snapshot. Such techniques will be discussed in the Some additional measures against forensics section of this guide.

Download Virtualbox and Whonix utilities:

You should download a few things within the host OS.

- The latest version of the Virtualbox installer according to your Host OS https://www.virtualbox.org/wiki/Downloads [Archive.org]
- (Skip this if you cannot use Tor natively of through a VPN) The latest Whonix OVA file from https://www.whonix.org/wiki/Download [Archive.org] according to your preference (Linux/Windows, with a Desktop interface XFCE for simplicity or only with the text-client for advanced users)

This will conclude the preparations and you should now be ready to start setting up the final environment that will protect your anonymity online.

---

[310] Oracle Virtualbox Manual, Snapshots https://docs.oracle.com/en/virtualization/virtualbox/6.0/user/snapshots.html [Archive.org]

[311] Utica College, FORENSIC RECOVERY OF EVIDENCE FROM DELETED ORACLE VIRTUALBOX VIRTUAL MACHINES https://programs.online.utica.edu/sites/default/files/Neal_6_Gonnella_Forensic_Recovery_of_Evidence_from_Deleted_Oracle_VirtualBox_Virtual_Machine.pdf [Archive.org]

Virtualbox Hardening recommendations:

For ideal security, you should follow the recommendations provided here for each Virtualbox Virtual Machine https://www.whonix.org/wiki/Virtualization_Platform_Security#VirtualBox_Hardening [Archive.org] :

- Disable Audio.
- Do not enable Shared Folders.
- Do not enable 2D acceleration. This one is done running the following command ```VBoxManage modifyvm "vm-id" --accelerate2dvideo on|off```
- Do not enable 3D acceleration.
- Do not enable the Serial Port.
- Remove the Floppy drive.
- Remove the CD/DVD drive.
- Do not enable the Remote Display server.
- Enable PAE/NX (NX is a security feature).
- Disable Advanced Configuration and Power Interface (ACPI). This one is done running the following command ```VBoxManage modifyvm "vm-id" --acpi on|off```
- Do not attach USB devices.
- Disable the USB controller which is enabled by default. Set the Pointing Device to "PS/2 Mouse" or changes will revert.

Finally, also follow this recommendation to desync the clock you are your VM compared to your host OS https://www.whonix.org/wiki/Network_Time_Synchronization#Spoof_the_Initial_Virtual_Hardware_Clock_Offset [Archive org]

This offset should be within a 60000 milliseconds range and should be different for each VM and here are some examples (which can be later applied to any VM):

- ```VBoxManage modifyvm "Whonix-Gateway-XFCE" --biossystemtimeoffset -35017```
- ```VBoxManage modifyvm "Whonix-Gateway-XFCE" --biossystemtimeoffset +27931```
- ```VBoxManage modifyvm "Whonix-Workstation-XFCE" --biossystemtimeoffset -35017```
- ```VBoxManage modifyvm "Whonix-Workstation-XFCE" --biossystemtimeoffset +27931```

Also consider applying these mitigations from VirtualBox to mitigate Spectre[312]/Meltdown[313] vulnerabilities by running this command from the VirtualBox Program Directory. All of these are described here: https://www.whonix.org/wiki/Spectre_Meltdown [Archive.org] (be aware these can impact severely the performance of your VMs but should be done for best security).

Finally consider the security advice from Virtualbox themselves here https://www.virtualbox.org/manual/ch13.html [Archive org]

Tor over VPN:

Skip this step if you do not intend to use Tor over VPN and only intend to use Tor or cannot.

If you intend to use Tor over VPN for any reason. You first must configure a VPN service on your host OS.

Remember that in this case, I recommend having two VPN accounts. Both paid with cash/Monero (see Appendix O: Get an anonymous VPN/Proxy). One will be used in the Host OS for the first VPN connection. The other could be used in the VM to achieve VPN over Tor over VPN (User > VPN > Tor > VPN).

If you intend to only use Tor over VPN, you only need one VPN account.

See Appendix R: Installing a VPN on your VM or Host OS for instructions.

---

[312] Wikipedia, Spectre https://en.wikipedia.org/wiki/Spectre_(security_vulnerability) [Wikiless] [Archive org]

[313] Wikipedia, Meltdown https://en.wikipedia.org/wiki/Meltdown_(security_vulnerability) [Wikiless] [Archive.org]

Whonix Virtual Machines:

Skip this step if you cannot use Tor.

- Start Virtualbox on your Host OS.
- Import Whonix file Into Virtualbox following the instructions on https://www.whonix.org/wiki/VirtualBox/XFCE [Archive.org]
- Start the Whonix VMs

Remember at this stage that if you are having issues connecting to Tor due to censorship or blocking, you should consider connecting using Bridges as explained in this tutorial https://www.whonix.org/wiki/Bridges [Archive.org].

- Update the Whonix VMs by following the instructions on https://www.whonix.org/wiki/Operating_System_Software_and_Updates#Updates [Archive.org]
- Shutdown the Whonix VMs
- Take a Snapshot of the updated Whonix VMs within Virtualbox (select a VM and click the Take Snapshot button). More on that later.
- Go to next step

Important Note: You should also read these very good recommendations over there https://www.whonix.org/wiki/DoNot [Archive org] as most of those principles will also apply to this guide. You should also read their general documentation here https://www.whonix.org/wiki/Documentation [Archive org] which will also provide tons of advice like this guide.

Pick your guest workstation Virtual Machine:

Using Whonix/Linux will require more skills on your side as these are Linux distributions. You will also encounter more difficulties if you intend to use specific software that might be harder to use on Whonix/Linux. Setting up a VPN over Tor on Whonix will also be more complicated than on Windows as well.

If you can use Tor:

You can decide if you prefer to conduct your sensitive activities from the Whonix Workstation provided in the previous section **(highly recommended)** or from a Custom VM that will use the Whonix Gateway like the Whonix Workstation (less secure but might be required depending on what you intend to do).

If you cannot use Tor:

If you cannot use Tor, you can use a Custom VM of your choice that will ideally use an anonymous VPN, if possible, to then connect to the Tor network. Or you could go with the risky route: See Appendix P: Accessing the internet as safely as possible when Tor and VPNs are not an option

Linux Virtual Machine (Whonix or Linux):

Whonix Workstation (recommended and preferred):

Skip this step if you cannot use Tor.

Just use the provided Whonix Workstation VM. **It is the safest and most secure way to go in this route.**

It is also the only VM that will provide Stream Isolation pre-configured for most apps by default[314].

If you want additional software on the Workstation (such as another Browser), follow their guide here https://www.whonix.org/wiki/Install_Software [Archive.org]

Consider running Whonix in Live Mode if for extra malware protection, See https://www.whonix.org/wiki/Anti-Forensics_Precautions [Archive.org]

Do not forget to apply the VM hardening recommendations here: Virtualbox Hardening recommendations.

Consider using AppArmor on your Whonix Workstations by following this guide: https://www.whonix.org/wiki/AppArmor [Archive.org]

---

[314] Whonix Documentation, Stream Isolation, By Settings https://www.whonix.org/wiki/Stream_Isolation#By_Settings [Archive.org]

Linux (any distro):

Be careful, any customization you make to the non-Whonix guest VMs (keyboard layout, language, time zone, screen resolution or other) could be used to fingerprint your VMs later. See https://www.whonix.org/wiki/VM_Fingerprinting [Archive.org]

If you can use Tor (natively or over a VPN):

Use the Linux Distro of your choice. Personally, I would recommend Ubuntu or Fedora for convenience but any other would work too. Be sure to not enable any telemetry.

Refer to this tutorial https://www.whonix.org/wiki/Other_Operating_Systems [Archive.org] for detailed instructions.

Consider hardening the VM as recommended in Hardening Linux.

If you cannot use Tor:

Use the Linux Distro of your choice. Personally, I would recommend Ubuntu or Fedora for convenience but any other would work too. Be sure to not enable any telemetry. You could go with the risky route: See Appendix P: Accessing the internet as safely as possible when Tor and VPNs are not an option

Windows 10 Virtual Machine:

Be careful, any customization you make to the non-Whonix guest VMs (keyboard layout, language, time zone, screen resolution or other) could be used to fingerprint your VMs later. See https://www.whonix.org/wiki/VM_Fingerprinting [Archive.org]

Windows 10 ISO download:

You have two choices here:

- Go with the Official Windows 10 Pro VM and harden it yourself: see Appendix C: Windows Installation Media Creation and go with the ISO route.
- Go with Windows AME (Ameliorated) from the https://ameliorated.info/ [Archive.org] project which is a special Windows 10 build stripped from all telemetry/advertising and update components. **Note that you will not be able to update this version with the latest security patched and will have to just re-download a new release. See Appendix Y: Windows AME installation**

If you can use Tor (natively or over a VPN):

Refer to this tutorial https://www.whonix.org/wiki/Other_Operating_Systems [Archive.org] for detailed instructions.

Install:

- Shutdown the Whonix Gateway VM (this will prevent Windows from sending out telemetry and allow you to create a local account).
- Open Virtualbox
- Select Machine > New > Select Windows 10 64bit
- Allocate a minimum amount of 2048MB but ideally 4096MB if your Ram allows it
- Create a Virtual Disk using the VDI format and select Dynamically Allocated
- Keep the disk size at 50GB (this is a maximum; it should not reach that much)
- Select the VM and click Settings, Go into the Network Tab
- Select "Internal Network" in the "Attached to" Field and select Whonix.
- Go into the Storage Tab, Select the Empty CD and click the icon next to SATA Port 1
- Click on "Choose a disk file" and select the Windows ISO you previously downloaded
- Click ok and start the VM
- Virtualbox will prompt you to select a Starting disk (the ISO file), select it and click Start
- Follow the Steps according to your choice for Windows:
    - Appendix A: Windows Installation
    - Appendix Y: Windows AME installation
- Start the Whonix Gateway VM

Network Settings:

- Go back into Settings then Network & Internet
- Click Properties (Below Ethernet)
- Edit IP settings:
- Enable IPv4 and set the following:
    - IP address ```10.152.152.50``` (increase this IP by 1 for any other VM)
    - Subnet prefix length ```18``` (```255.255.192.0```)
    - Gateway ```10.152.152.10``` (this is the Whonix Gateway)
    - DNS ```10.152.152.10``` (this is again the Whonix Gateway)
    - Save
- Windows might prompt you if you want to be "discoverable" on this network. Click NO.

Every time you will power on this VM in the future, make sure you change its Ethernet Mac Address before each boot. You can do this in Virtualbox > Settings > Network > Advanced > Click the refresh button next to the MAC address. You can only do this while the VM is powered off.

Choose a browser within the VM:

Check: Appendix V: What browser to use in your Guest VM/Disposable VM

Check:

If you cannot use Tor:

See Appendix P: Accessing the internet as safely as possible when Tor and VPNs are not an option

Install:

- Open Virtualbox
- Select Machine > New > Select Windows 10 64bit
- Allocate a minimum amount of 2048MB but ideally 4096MB if your Ram allows it
- Create a Virtual Disk using the VDI format and select Dynamically Allocated
- Keep the disk size at 50GB (this is a maximum; it should not reach that much)
- Go into the Storage Tab, Select the Empty CD and click the icon next to SATA Port 1
- Click on "Choose a disk file" and select the Windows ISO you previously downloaded
- Click ok and start the VM
- Virtualbox will prompt you to select a Starting disk (the ISO file), select it and click Start
- Follow the Steps in Appendix A: Windows Installation

Network Settings:

- Windows will prompt you if you want to be "discoverable" on this network. Click NO.

Every time you will power on this VM in the future, make sure you change its Ethernet Mac Address before each boot. You can do this in Virtualbox > Settings > Network > Advanced > Click the refresh button next to the MAC address. You can only do this while the VM is powered off.

Choose a browser within the VM:

This time, I will recommend Brave browser.

See why here: Appendix V: What browser to use in your Guest VM/Disposable VM

If you want to use Brave:

- Download and install Brave browser from https://brave.com/download/ [Archive org]
- Open Brave Browser
- Go into "Settings"
- Go into "Shields"
- Set "Trackers and Ads blocking" to "Aggressive"
- Set "Upgrade to HTTPS" to enabled
- Set Fingerprinting blocking to "Standard"

- Go into "Clear Browsing Data"
- Select "On Exit"
- Check all options
- Do Not Enable Brave Rewards

Only use Private Windows no matter what Browser you picked.

Additional Privacy settings in Windows 10:
Skip these if you used Windows AME from https://ameliorated.info/ [Archive.org]

See Appendix B: Windows Additional Privacy Settings

Android Virtual Machine:

Because sometimes you want to run mobile Apps anonymously too. You can also set-up an Android VM for this purpose. As in other cases, ideally this VM will also be sitting behind the Whonix Gateway for Tor network connectivity. But this can also be set-up as VPN over Tor over VPN

If you can use Tor (natively or over a VPN):
Later in the VM settings during creation, go into Network and select Internal Network, Whonix.

Then on Android itself:

- Select Wi-Fi
- Select VirtWifi to connect
- Go into the advanced Wi-Fi properties
- Switch from DHCP to Static
    - IP address ```10.152.152.50``` (increase this IP by 1 for any other VM)
    - Subnet prefix length ```18``` (```255.255.192.0```)
    - Gateway ```10.152.152.10``` (this is the Whonix Gateway)
    - DNS ```10.152.152.10``` (this is again the Whonix Gateway)

If you cannot use Tor:
Just use the tutorials as is and see Appendix P: Accessing the internet as safely as possible when Tor and VPNs are not an option

Installation:
Basically, follow the tutorial here: https://www.android-x86.org/documentation/virtualbox.html [Archive.org]

- Download the appropriate ISO file, personally, I recommend the CM 14.1 (based on old Android 7 "Nougat") as it was the snappier in my tests.
- Create a New VM.
- Select Linux and Linux 2.6 / 3.x / 4.x 64 Bit.
- In System:
    - Allocate at least 2048MB (2GB) memory
    - Uncheck the Floppy drive
    - In the Processor Tab, select at least 1 or more CPUs
    - Enable PAE/NX
- In Display Settings, Change the adapter to VBoxVGA
- In Audio Settings, Change to Intel HD Audio
- Start the VM
- Select Advanced if you want persistence, Live if you want a disposable Boot (and skip the next steps).
- Select Auto Install on Selected Hard Disk
- Select Run Android
- Setup as you wish (disable all prompts for data collections). **I recommend using the TaskBar Home.**
- Go into Settings, Android-x86 Options and disable all collection.
- Connect to VirtWifi Wi-Fi Network **(see the above section if you are behind Whonix and want to use Tor)**

You are now done and can now install any Android app.

MacOS Virtual Machine:

Yes, you can actually run MacOS within Virtualbox (on Windows/Linux/MacOS host systems) if you really want to use MacOS. You can run any version of MacOS you want.

If you can use Tor (natively or over a VPN):

During the following tutorials, before starting the MacOS VM, make sure you do put the MacOS VMs on the Whonix Network.

- Select the VM and click Settings, Go into the Network Tab
- Select "Internal Network" in the "Attached to" Field and select Whonix

Afterward, and during the install, you will need to input an IP address manually to connect through the Whonix Gateway.

Use these settings when prompted in the MacOS installation process:

  - IP address ```10.152.152.50``` (increase this IP by 1 for any other VM)
  - Subnet prefix length ```18``` (```255.255.192.0```)
  - Gateway ```10.152.152.10``` (this is the Whonix Gateway)
  - DNS ```10.152.152.10``` (this is again the Whonix Gateway)

If you cannot use Tor:

Just use the tutorials as is and see Appendix P: Accessing the internet as safely as possible when Tor and VPNs are not an option

Installation:

- Windows Host OS:
  - Virtualbox Catalina Tutorial: https://www.wikigain.com/install-macos-catalina-on-virtualbox-on-windows/ [Archive.org]
  - Virtualbox Big Sur Tutorial: https://www.wikigain.com/how-to-install-macos-big-sur-on-virtualbox-on-windows-pc/ [Archive.org]
- MacOS Host OS:
  - Just use the same tutorials as above but execute the various commands in terminal. It should work without issue.
- Linux Host OS:
  - Just use the same tutorials as above but execute the various commands in terminal. It should work without issue.

There are some drawbacks with running MacOS on Virtual Machines. The main one is that they do not actually have a serial number (0 by default) and you will be unable to log-in into any Apple provided service (iCloud, iMessage…) without a genuine ID. You can set such IDs using this script: https://github.com/myspaghetti/macos-virtualbox [Archive org] but keep in mind randomly generated IDs will not work and using the ID of someone else will break their Terms of Services and could count as impersonation (and therefore could be illegal).

Note: I also ran in multiple issues with running these on AMD processors. This can be fixed so here is the configuration I used which worked fine with Catalina and Big Sur which will tell Virtualbox to emulate an Intel Processor instead:

- ```VBoxManage modifyvm "MacOSCatalina" –-cpuidset 00000001 000106e5 00100800 0098e3fd bfebfbff```
- ```VBoxManage setextradata "MacOSCatalina" "VBoxInternal/Devices/efi/0/Config/DmiSystemProduct" "MacBookPro15,1" ```
- ```VBoxManage setextradata "MacOSCatalina" "VBoxInternal/Devices/efi/0/Config/DmiBoardProduct" "Mac-551B86E5744E2388"```
- ```VBoxManage setextradata "MacOSCatalina" "VBoxInternal/Devices/smc/0/Config/DeviceKey" "ourhardworkbythesewordsguardedpleasedontsteal(c)AppleComputerInc"```

- ```VBoxManage setextradata "MacOSCatalina" "VBoxInternal/Devices/smc/0/Config/GetKeyFromRealSMC" 1```
- ```VBoxManage modifyvm "MacOSCatalina" --cpu-profile "Intel Core i7-6700K"````
- ```VBoxManage setextradata "MacOSCatalina" VBoxInternal2/EfiGraphicsResolution 1920x1080```

Hardening MacOS:

Refer to Hardening MacOS.

KeepassXC:

You will need something to store your data (logins/passwords, identities and TOTP[315] information).

For this purpose, I strongly recommend KeePassXC because of their integrated TOTP feature. This is the ability to create entries for 2FA[316] authentication with the authenticator feature.

Remember this should ideally be installed on your Guest VM and not on your Host OS. You should never do any sensitive activities from your Host OS.

Here are the tutorials:

- Tails: KeePassXC is integrated by default
- Whonix: https://www.whonix.org/wiki/KeePassXC [Archive.org]
- Linux:
  - Download from https://keepassxc.org/download/ [Archive org]
  - Follow the tutorial here https://keepassxc.org/docs/KeePassXC_GettingStarted.html#_linux [Archive.org]
- Windows:
  - Download from https://keepassxc.org/download/ [Archive org]
  - Follow the tutorial here https://KeePassXC.org/docs/KeePassXC_GettingStarted.html#_microsoft_windows [Archive.org]
- MacOS:
  - Download from https://keepassxc.org/download/ [Archive org]
  - Follow the tutorial here https://keepassxc.org/docs/KeePassXC_GettingStarted.html#_macos [Archive org]

Test that KeePassXC is working before going to next step.

VPN client installation (cash/Monero paid):

If you decided to not use a cash-paid VPN and just want to use Tor, skip this step.

If you cannot use a VPN at all in a hostile environment, skip this step.

Otherwise, see Appendix R: Installing a VPN on your VM or Host OS to install a VPN client on your client VM.

This should conclude the Route and you should now be ready.

About VPN Client Data Mining/Leaks:

You might be asking yourself if those VPN clients are trustworthy not to leak any information about your local environment to the VPN provider when using them in the "VPN over Tor" context.

This is a valid concern but should be taken with a grain of salt.

Remember that all VPN activities are happening from a sandboxed VM on an internal network behind a Network Gateway (the Whonix Gateway). It does not matter much if the VPN client leaves some identifiers on your guest VM. The guest VM is still sandboxed and walled-off from the Host OS. The attack surface is pretty small IMHO especially when using the reputable and recommended VPN providers within the guides (iVPN, Mullvad, ProtonVPN).

---

[315] Wikipedia, TOTP https://en.wikipedia.org/wiki/Time-based_One-time_Password_algorithm [Wikiless] [Archive.org]

[316] Wikipedia, Multi-Factor Authentication https://en.wikipedia.org/wiki/Multi-factor_authentication [Wikiless] [Archive.org]

At best, the VPN client would know your local IP (internal IP) and some randomized identifies but should not be able to get anything from the Host OS. And in theory, the VPN client should not send any telemetry back to the VPN provider. If your VPN client does this or ask this. You should consider changing provider.

(Optional) Allowing only the VMs to access the internet while cutting off the Host OS to prevent any leak:

This step will allow you to configure your Host OS so that only the Whonix Gateway VM will have access to the internet. This will therefore prevent any "leak" from your Host OS while letting the Whonix Gateway establish the tor connectivity. The other VMs (Whonix Workstation or any other VM you installed behind it will not be affected)

There are three ways to do this:

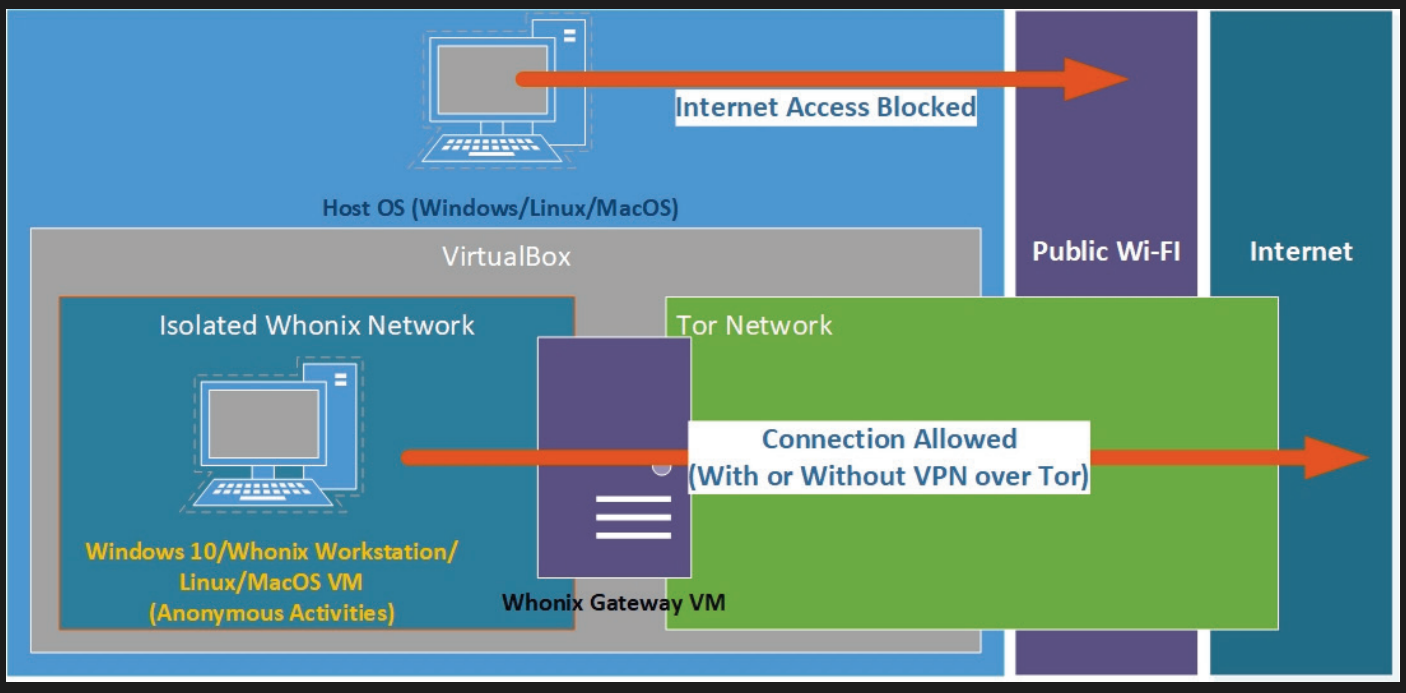
- The Lazy Way (not really recommended): not supported by Whonix and might have some security implication as you will expose the Whonix Gateway VM to the Public Wi-Fi network. I would advise against this unless you are in a hurry or very lazy.
    - **This method will not work with Wi-Fi captive portals requiring any registration to connect.**
- The Better Way (see further down): still not supported by Whonix but it will not expose the Whonix Gateway VM to the Public Wi-Fi network. This should keep things in check in terms of security.
- The Best Way: Using an external USB Wi-Fi dongle and just disabling Wi-Fi on the Host OS/Computer.

*The Lazy Way (**not supported by Whonix** but it will work if you are in a hurry, see further for the better way):*

This way is not supported by the Whonix project[317] but I will go ahead and give this option anyway. IMHO this is helpful to prevent your Host OS from leaking any information while you are using the Whonix VMs.

Note that this option as-is will only work on Wi-Fis without a captive portal (where you must enter some information to unlock access).

The illustration below shows the result of this step:



Configuration of the Whonix Gateway VM:

For this to work we will need to change some configuration on the Whonix Gateway VM. Mainly we will need to add a DHCP client to the Whonix Gateway to receive IP addresses from the network. To do those change the Host OS will still have to have internet access allowed for now.

So here is how:

[317] Whonix Documentation, Bridged Adapters Warning https://www.whonix.org/wiki/Whonix-Gateway_Security#Warning:_Bridged_Networking [Archive org]

- Be sure to have your Host OS connected to a safe Wi-Fi.
- Through VirtualBox, start the Whonix Gateway VM
- Start a Terminal on the VM
- Install a DHCP client on the Whonix Gateway VM using the following command:
  - ```sudo apt install dhcpcd5```
- Now edit the Whonix Gateway VM network configuration using the following command:
  - ```sudo nano /etc/network/interfaces.d/30_non-qubes-whonix```
- Within the file change the following lines:
  - ```# auto eth0``` to ```auto eth0```
  - ```# iface eth0 inet dhcp``` to ```iface eth0 inet dhcp```
  - ```iface eth0 inet static``` to ```# iface eth0 inet static```
  - ``` address 10.0.2.15``` to ```# address 10.0.2.15```
  - ``` netmask 255.255.255.0``` to ```# netmask 255.255.255.0```
  - ``` gateway 10.0.2.2``` to ```# gateway 10.0.2.2```
- Save (using Ctrl+X and confirm with Y) and power off the VM from the top left menu
- Go in to the VirtualBox Application and select the Whonix Gateway VM
- Click Settings
- Click the Network Tab
- For Adapter 1, change the "Attached To" value from "NAT" to "Bridged Adapter"
- As "Name", select your Wi-Fi network Adapter
- Click OK and you are done with the VM configuration part

Configuration of the Host OS:

Now we must block internet access from your Host OS while still allowing the VM to connect. This will be done by connecting to a Wi-Fi with the Host OS but without assigning itself an IP address. The VM will then use your Wi-fi association to get an IP address.

Windows Host OS:

The goal here is to associate to a Wi-Fi network without having an internet connection. We will achieve this by deleting the Gateway from the connection after you are connected.

- First connect to the safe Wi-Fi of your choice
- Open an administrative command prompt (right click on Command Prompt and Run as Administrator)
- Run the following command: ```route delete 0.0.0.0``` (this deletes the Gateway from your IP configuration)
- You are done, your Host OS will now be unable to access the internet while still connected to the Wi-Fi
  - Note that this will reset at each disconnect/reconnection to a network and you will have to delete the route again. This is not permanent.
- You can now start the Whonix Gateway VM which should now obtain an IP automatically from the Wi-Fi network and should provide Network to the other VMs behind (Whonix Workstation or other).
- And finally, after that you can start the Whonix Workstation VM (or any other VM you configured to work behind the Whonix Gateway VM) and it should be connected to the internet through Tor.

Linux Host OS:

The goal here is to associate to a Wi-Fi network without having an internet connection. We will achieve this by deleting the Gateway from the connection after you are connected.

- First connect to the safe Wi-Fi of your choice
- Open a Terminal
- Run the following command: ```sudo ip route del default``` (this deletes the Gateway from your IP configuration)
- You are done, your Host OS will now be unable to access the internet while still connected to the Wi-Fi
  - Note that this will reset at each disconnect/reconnection to a network and you will have to delete the route again. This is not permanent.

- You can now start the Whonix Gateway VM which should now obtain an IP automatically from the Wi-Fi network and should provide Network to the other VMs behind (Whonix Workstation or other).
- And finally, after that you can start the Whonix Workstation VM (or any other VM you configured to work behind the Whonix Gateway VM) and it should be connected to the internet through Tor.

MacOS Host OS:

The goal here is to associate to a Wi-Fi network without having an internet connection. We will achieve this by deleting the Gateway from the connection after you are connected.

- First connect to the safe Wi-Fi of your choice
- Open a Terminal
- Run the following command: ```sudo route delete default``` (this deletes the Gateway from your IP configuration)
- You are done, your Host OS will now be unable to access the internet while still connected to the Wi-Fi
    - Note that this will reset at each disconnect/reconnection to a network and you will have to delete the route again. This is not permanent.
- You can now start the Whonix Gateway VM which should now obtain an IP automatically from the Wi-Fi network and should provide Network to the other VMs behind (Whonix Workstation or other).
- And finally, after that you can start the Whonix Workstation VM (or any other VM you configured to work behind the Whonix Gateway VM) and it should be connected to the internet through Tor.

The Better Way (recommended):

This way will not go against Whonix recommendations (as it will not expose the Whonix Gateway to the Host OS) and will have the advantage of allowing connections not only to open Wi-Fis but also to the ones with a Captive Portal where you need to enter some information to access the internet.

Yet this will still not be supported by the Whonix project but I think it is fine as the main concern for the previous Lazy Way is to have the Whonix Gateway VM exposed to the Host Network and it will not be the case here.

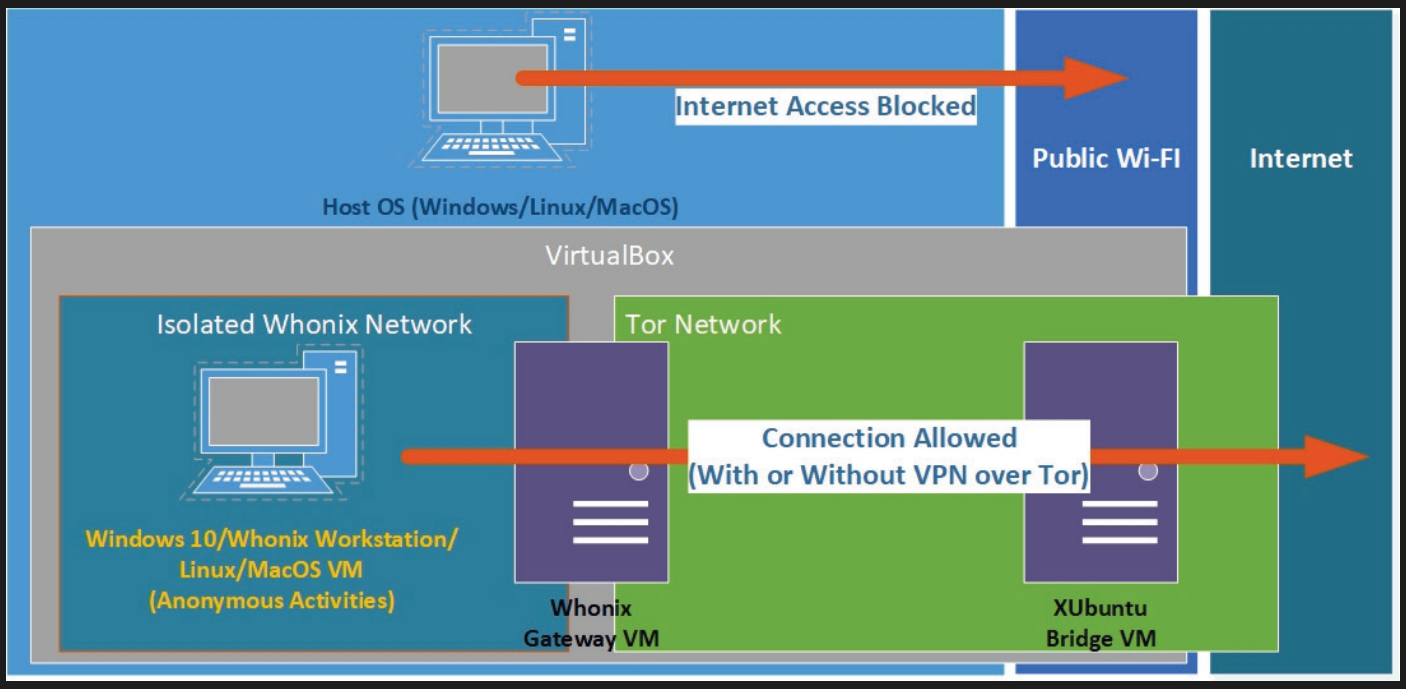
This option will require an additional VM between the Host OS and the Whonix Gateway to act as a Network Bridge.

For this purpose, I will recommend the use of a lightweight Linux Distro. Any will do but the easiest IMHO will be an Ubuntu based and I would recommend the lightweight XUbuntu as it will be extremely easy to configure this setup.

Why XUbuntu and not Ubuntu or KUbuntu? Because XUbuntu uses XFCE desktop environment which is lightweight and this VM will only serve as a proxy and nothing else.

Of course, you can also achieve this with any other Linux distro if you so decide you do not like XUbuntu.

This is how it will look at the end:



Installing XUbuntu VM:

Make sure you are connected to a safe Wi-Fi for this operation.

First you will need to download the latest XUbuntu Stable release ISO from https://xubuntu.org/download/

When you are done with the download, it is time to create a new VM.

- Start VirtualBox Manager
- Create a new VM and name it as you want, for example "XUbuntu Bridge"
- Select type "Linux"
- Select Version "Ubuntu (64-bit)"
- Leave other options to default and click Create
- On the next screen, leave the default options and click Create
- Select the newly create VM and click Settings
- Select Network
- For Adapter 1, Switch to Bridged Mode and pick your Wi-Fi adapter in the Name
- Select Adapter 2 and enable it
- Attach it to "Internal Network" and name it "XUbuntu Bridge"
- Select Storage
- Select the Empty CD drive
- On the right side, Click the CD icon and select "Choose a disk file"
- Select the ISO of XUbuntu you previously downloaded and Click Ok
- Start the VM
- Select Start XUbuntu
- Select Install XUbuntu
- Pick your Keyboard Layout and click Continue
- Select Minimal Installation and Download Updates while install XUbuntu
- Select Erase Disk and install XUbuntu and click Install Now
- Select the Time Zone of your choice and click Continue
- Pick some random names unrelated to you (my favorite username is "NoSuchAccount")
- Pick a password and require password to login
- Click Continue and wait for the install to finish and Restart
- When you are done rebooting, log-in
- Click the upper right connection icon (it looks like 2 rotating spheres)
- Click Edit Connections

- Select Wired Connection 2 (Adapter 2 previously configured in VirtualBox settings)
- Select the IPv4 Tab
- Change the Method to "Shared to other computers" and click Save
- You are now done setting up the XUbuntu Bridge VM

Configuring the Whonix Gateway VM:

By default, the Whonix Gateway has no DHCP client and will require one to get an IP from a shared network you configured earlier.

- Through VirtualBox, start the Whonix Gateway VM
- Start a Terminal on the VM
- Install a DHCP client on the Whonix Gateway VM using the following command:
  - ```sudo apt install dhcpcd5```
- Now edit the Whonix Gateway VM network configuration using the following command:
  - ```sudo nano /etc/network/interfaces.d/30_non-qubes-whonix```
- Within the file change the following lines:
  - ```# auto eth0``` to ```auto eth0```
  - ```# iface eth0 inet dhcp``` to ```iface eth0 inet dhcp```
  - ```iface eth0 inet static``` to ```# iface eth0 inet static```
  - ``` address 10.0.2.15``` to ```# address 10.0.2.15```
  - ``` netmask 255.255.255.0``` to ```# netmask 255.255.255.0```
  - ``` gateway 10.0.2.2``` to ```# gateway 10.0.2.2```
- Save (using Ctrl+X and confirm with Y) and power off the VM from the top left menu
- Go in to the VirtualBox Application and select the Whonix Gateway VM
- Click Settings
- Click the Network Tab
- For Adapter 1, change the "Attached To" value from "NAT" to "Internal Network"
- As "Name", select the internal network "XUbuntu Bridge" you created earlier and click OK
- Reboot the Whonix Gateway VM
- From the upper left Menu, select System, Tor Control Panel, and check that you are connected (you should be)
- You are done configuring the Whonix Gateway VM

Configuration of the Host OS:

Now we must block internet access from your Host OS while still allowing the XUbuntu Bridge VM to connect. This will be done by connecting to a Wi-Fi with the Host OS but without assigning itself a gateway address. The VM will then use your Wi-fi association to get an IP address.

If necessary, from the XUbuntu Bridge VM, you will be able to launch a Browser to enter information into any captive/registration portal on the Wi-Fi network.

Only the XUbuntu Bridge VM should be able to access the internet. The Host OS will be limited to local traffic only.

Windows Host OS:

The goal here is to associate to a Wi-Fi network without having an internet connection. We will achieve this by deleting the Gateway from the connection after you are connected.

- First connect to the safe Wi-Fi of your choice
- Open an administrative command prompt (right click on Command Prompt and Run as Administrator)
- Run the following command: ```route delete 0.0.0.0``` (this deletes the Gateway from your IP configuration)
- You are done, your Host OS will now be unable to access the internet while still connected to the Wi-Fi
  - Note that this will reset at each disconnect/reconnection to a network and you will have to delete the route again. This is not permanent.
- You can now start the XUbuntu Bridge VM which should now obtain an IP automatically from the Wi-Fi network and should provide Network to the other VMs behind (Whonix Workstation or other).

- If Necessary, you can use the XUbuntu Bridge VM Browser to fill in any information on any captive/registration portal to access the Wi-Fi.
- After that you can start the Whonix Gateway VM which should obtain the Internet Connection from the XUbuntu Bridge VM.
- And finally, after that you can start the Whonix Workstation VM (or any other VM you configured to work behind the Whonix Gateway VM) and it should be connected to the internet through Tor.

Linux Host OS:

The goal here is to associate to a Wi-Fi network without having an internet connection. We will achieve this by deleting the Gateway from the connection after you are connected.

- First connect to the safe Wi-Fi of your choice
- Open a Terminal
- Run the following command: ```sudo ip route del default``` (this deletes the Gateway from your IP configuration)
- You are done, your Host OS will now be unable to access the internet while still connected to the Wi-Fi
    - Note that this will reset at each disconnect/reconnection to a network and you will have to delete the route again. This is not permanent.
- You can now start the XUbuntu Bridge VM which should now obtain an IP automatically from the Wi-Fi network and should provide Network to the other VMs behind (Whonix Workstation or other).
- If Necessary, you can use the XUbuntu Bridge VM Browser to fill in any information on any captive/registration portal to access the Wi-Fi.
- After that you can start the Whonix Gateway VM which should obtain the Internet Connection from the XUbuntu Bridge VM.
- And finally, after that you can start the Whonix Workstation VM (or any other VM you configured to work behind the Whonix Gateway VM) and it should be connected to the internet through Tor.

MacOS Host OS:

The goal here is to associate to a Wi-Fi network without having an internet connection. We will achieve this by deleting the Gateway from the connection after you are connected.

- First connect to the safe Wi-Fi of your choice
- Open a Terminal
- Run the following command: ```sudo route delete default``` (this deletes the Gateway from your IP configuration)
- You are done, your Host OS will now be unable to access the internet while still connected to the Wi-Fi
    - Note that this will reset at each disconnect/reconnection to a network and you will have to delete the route again. This is not permanent.
- You can now start the XUbuntu Bridge VM which should now obtain an IP automatically from the Wi-Fi network and should provide Network to the other VMs behind (Whonix Workstation or other).
- If Necessary, you can use the XUbuntu Bridge VM Browser to fill in any information on any captive/registration portal to access the Wi-Fi.
- After that you can start the Whonix Gateway VM which should obtain the Internet Connection from the XUbuntu Bridge VM.
- And finally, after that you can start the Whonix Workstation VM (or any other VM you configured to work behind the Whonix Gateway VM) and it should be connected to the internet through Tor.

The best way:

This way will not go against Whonix recommendations (as it will not expose the Whonix Gateway to the Host OS) and will have the advantage of allowing connections not only to open Wi-Fis but also to the ones with a Captive Portal where you need to enter some information to access the internet. Yet this will still not be supported by the Whonix project but I think it is fine as the main concern for the previous Lazy Way is to have the Whonix Gateway VM exposed to the Host Network and it will not be the case here. This option is the best because the network will be completely disabled on the Host OS from booting up.

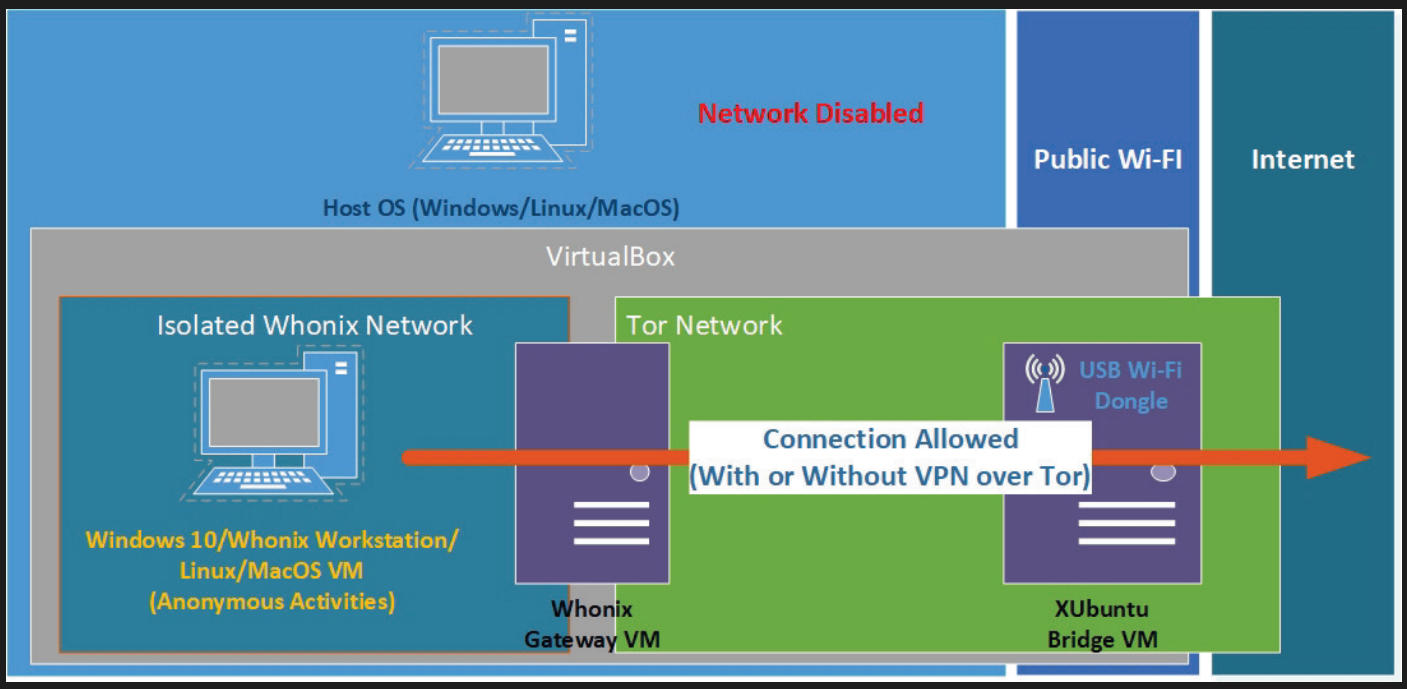
This option will require an additional VM between the Host OS and the Whonix Gateway to act as a Network Bridge and to connect to the Wi-Fi network. **This option requires a working USB Wi-Fi Dongle that will be passed-through to a bridge VM.**

For this purpose, I will recommend the use of a lightweight Linux Distro. Any will do but the easiest IMHO will be an Ubuntu based and I would recommend the lightweight XUbuntu as it will be extremely easy to configure this setup.

Why XUbuntu and not Ubuntu or KUbuntu? Because XUbuntu uses XFCE desktop environment which is lightweight and this VM will only serve as a proxy and nothing else.

Of course, you can also achieve this with any other Linux distro if you so decide you do not like XUbuntu.

This is how it will look at the end:



Configuration of the Host OS:

- Disable Networking on your Host OS completely (Turn off the on-board Wi-Fi completely)
- Plug-in and install your USB Wi-Fi Dongle. Connect it to a safe Public Wi-Fi. This should be easy and automatically installed by any recent OS (Windows 10, MacOS, Linux).

Configuring the Whonix Gateway VM:

By default, the Whonix Gateway has no DHCP client and will require one to get an IP from a shared network you will configure later, on a Bridge VM.

- Through VirtualBox, start the Whonix Gateway VM
- Start a Terminal on the VM
- Install a DHCP client on the Whonix Gateway VM using the following command:
  - ```sudo apt install dhcpcd5```
- Now edit the Whonix Gateway VM network configuration using the following command:
  - ```sudo nano /etc/network/interfaces.d/30_non-qubes-whonix```
- Within the file change the following lines:
  - ```# auto eth0``` to ```auto eth0```
  - ```# iface eth0 inet dhcp``` to ```iface eth0 inet dhcp```
  - ```iface eth0 inet static``` to ```# iface eth0 inet static```
  - ``` address 10.0.2.15``` to ```# address 10.0.2.15```
  - ``` netmask 255.255.255.0``` to ```# netmask 255.255.255.0```
  - ``` gateway 10.0.2.2``` to ```# gateway 10.0.2.2```
- Save (using Ctrl+X and confirm with Y) and power off the VM from the top left menu

Installing XUbuntu VM:

Make sure you are connected to a safe Wi-Fi for this operation.

First you will need to download the latest XUbuntu Stable release ISO from https://xubuntu.org/download/

When you are done with the download, it is time to create a new VM.

- Disconnect your Host OS from the Wi-Fi you previously connected to with the dongle and forget the network.
- Start VirtualBox Manager
- Create a new VM and name it as you want, for example "XUbuntu Bridge"
- Select type "Linux"
- Select Version "Ubuntu (64-bit)"
- Leave other options to default and click Create
- On the next screen, leave the default options and click Create
- Select the newly create VM and click Settings
- Select Network
- For Adapter 1, Attach it to "Internal Network" and name it "XUbuntu Bridge"
- Select Storage
- Select the Empty CD drive
- On the right side, Click the CD icon and select "Choose a disk file"
- Select the ISO of XUbuntu you previously downloaded and Click Ok
- Select the USB Tab
- On the right side, click the USB icon with a + sign (the second from the top)
- Select the Wi-Fi Adapter Dongle from the list and make sure it is checked (leave the USB options to default)
- Start the VM
- Select Start XUbuntu
- Select Install XUbuntu
- Pick your Keyboard Layout and click Continue
- Select Minimal Installation and do not check the Download Updates during install option
- Select Erase Disk and install XUbuntu and click Install Now
- Select the Time Zone of your choice and click Continue
- Pick some random names unrelated to you (my favorite username is "NoSuchAccount")
- Pick a password and require password to login
- Click Continue and wait for the install to finish and Restart
- When you are done rebooting, log-in
- Click the upper right connection icon (it looks like 2 rotating spheres)
- Click Edit Connections
- Select Wired Connection 1 (normally there should only be one)
- Select the IPv4 Tab
- Change the Method to "Shared to other computers" and click Save
- Again, click the upper right connection icon
- Connect to the safe Wi-Fi of your choice and if necessary, input the necessary information into a Captive Portal.
- You are now done setting up the XUbuntu Bridge VM

At this stage your Host OS should have no network at all and your XUbuntu VM should have a fully working Wi-Fi connection and this Wi-Fi connection will be shared to the Internal Network "XUbuntu Bridge".

Additional configuration the Whonix Gateway VM:

Now it is time to configure the Whonix Gateway VM to get access from the shared network from the bridge VM we just made on the previous step.

- Go in to the VirtualBox Application and select the Whonix Gateway VM

- Click Settings
- Click the Network Tab
- For Adapter 1, change the "Attached To" value from "NAT" to "Internal Network"
- As "Name", select the internal network "XUbuntu Bridge" you created earlier and click OK
- Reboot the Whonix Gateway VM
- From the upper left Menu, select System, Tor Control Panel, and check that you are connected (you should be)
- You are done configuring the Whonix Gateway VM

At this stage, your Whonix Gateway VM should be getting the internet access from the XUbuntu Bridge VM which in turn is getting internet access from the Wi-Fi Dongle and sharing it. Your Host OS should have no network connectivity at all.

All the VMs behind the Whonix Gateway should now work fine without additional configuration.

Final step:

Take a post-install VirtualBox snapshot of your VMs.

You are done and can now skip the rest to go to the Getting Online part.

The Qubes Route:

As they say on their own website, Qubes OS is a reasonably secure, free, open-source and security-oriented operating system for single-user desktop computing. Qubes OS leverages and extensively uses Xen-based virtualization to allow for the creation and management of isolated compartments called qubes.

Qubes OS is not a Linux distribution[318] but a Xen distribution. It is different from Linux distributions because it will make extensive use of Virtualization and Compartmentalization so that any app will run in a different VM (qube). As a bonus, Qubes OS integrates Whonix by default and allows for increased privacy and anonymity. It is highly recommended that you document yourself over Qubes OS principles prior to going this route. Here are some recommended resources:

- Qubes OS Introduction, https://www.qubes-os.org/intro/ [Archive org]
- Qubes OS Video Tours, https://www.qubes-os.org/video-tours/ [Archive.org]
- Qubes OS Getting Started, https://www.qubes-os.org/doc/getting-started/ [Archive.org]
- YouTube, Life Behind the Tinfoil: A Look at Qubes and Copperhead - Konstantin Ryabitsev, The Linux Foundation https://www.youtube.com/watch?v=8cU4hQg6GvU [Invidious]
- YouTube, I used the reasonably-secure Qubes OS for 6 months and survived - Matty McFatty [@themattymcfatty] https://www.youtube.com/watch?v=sbN5Bz3v-uA [Invidious]
- YouTube, Qubes OS: How it works, and a demo of this VM-centric OS https://www.youtube.com/watch?v=YPAvoFsvSbg [Invidious]

This OS is recommended by prominent figures such as Edward Snowden and Privacytools.io.

Qubes is the best option in this guide for people who are more comfortable with Linux and tech in general. But it has some downsides such as the lack of OS wide plausible deniability, its hardware requirements, and its hardware compatibility. While you can run this on 4GB of RAM as per their requirements[319], the recommended RAM is 16GB. I would advise against using Qubes OS if you have less than 8GB of RAM. If you want a comfortable experience, you should have 16GB, if you want a very good experience, you should have 24GB or 32GB.

The reason for this RAM requirement is that each app will run in a different VM and each of those VM will require and allocate a certain amount of memory that will not be available for other apps. If you are running native Windows apps within Qubes OS qubes, the ram overhead will be significant.

---

[318] Qubes OS, FAQ, https://www.qubes-os.org/faq/#is-qubes-just-another-linux-distribution [Archive.org]

[319] Qubes OS, System Requirements https://www.qubes-os.org/doc/system-requirements/ [Archive.org]

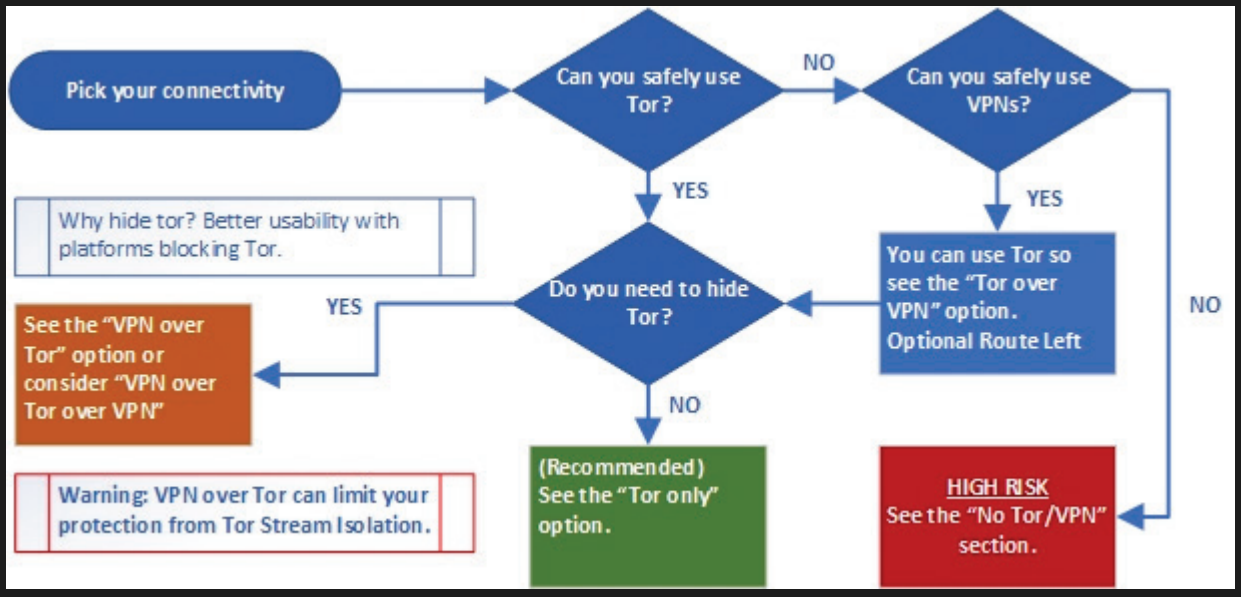
You should also check their hardware compatibility here https://www.qubes-os.org/hcl/ [Archive.org] before proceeding. Your mileage might vary and you might experience several issues with regards to hardware compatibility that you will have to troubleshoot and solve yourself.

I think that if you can afford it and are comfortable with the idea of using Linux, you should go with this route as it is probably the best one in terms of security and privacy. The only disadvantage of this route is that it does not provide a way to enable OS wide plausible deniability[272] unlike the Whonix route.

Pick your connectivity method:

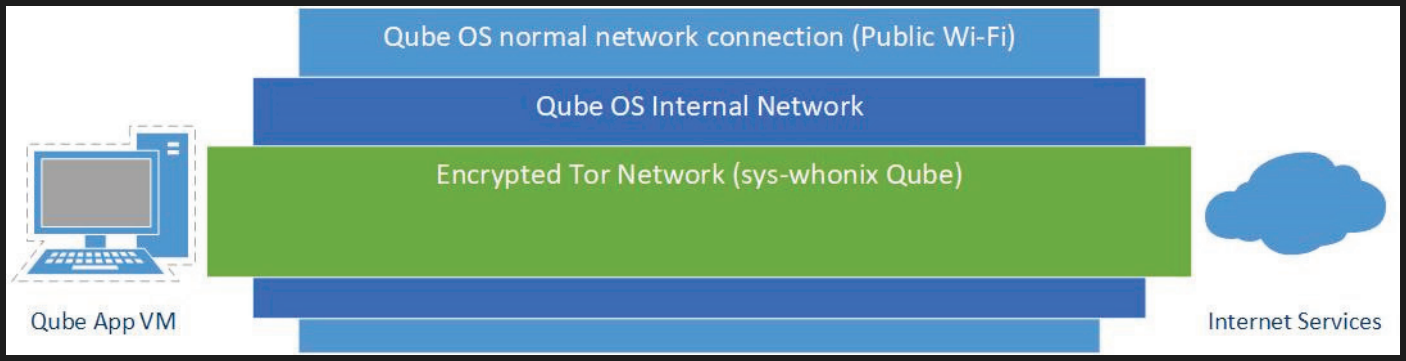
There are 7 possibilities within this route:

- **Recommended and preferred:**
  - **Use Tor alone (User > Tor > Internet)**
  - **Use VPN over Tor (User > Tor > VPN > Internet) in specific cases**
- Possible if required by context:
  - Use VPN over Tor over VPN (User > VPN > Tor > VPN > Internet)
  - Use Tor over VPN (User > VPN > Tor > Internet)
- Not recommended and risky:
  - Use VPN alone (User > VPN > Internet)
  - Use VPN over VPN (User > VPN > VPN > Internet)
- **Not recommended and highly risky (but possible)**
  - No VPN and no Tor (User > Internet)



Tor only:

This is the preferred and most recommended solution.



With this solution, all your network goes through Tor and it should be sufficient to guarantee your anonymity in most cases.

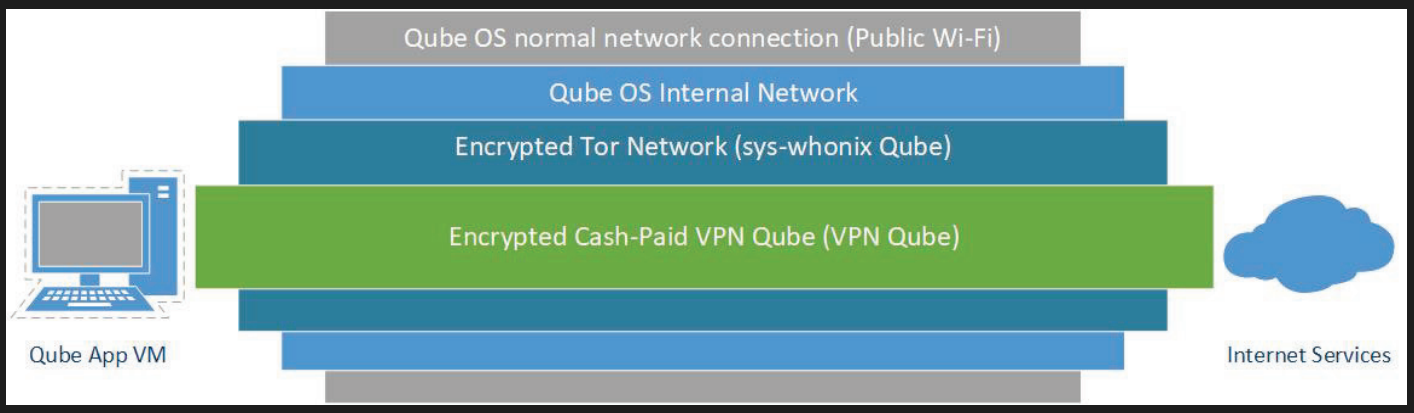
There is one main drawback tho: **Some services block/ban Tor Exit nodes outright and will not allow account creations from those.**

To mitigate this, you might have to consider the next option: VPN over Tor but consider some risks associated with it explained in the next section.

VPN/Proxy over Tor:

This solution can bring some benefits in some specific cases vs using Tor only where accessing the destination service would be impossible from a Tor Exit node. This is because many services will just outright ban, hinder, or block Tor (see https://gitlab.torproject.org/legacy/trac/-/wikis/org/doc/ListOfServicesBlockingTor [Archive.org]).

As you can see in this illustration, if your cash (preferred)/Monero paid VPN/Proxy is compromised by an adversary (despite their privacy statement and no-logging policies), they will only find an anonymous cash/Monero paid VPN account connecting to their services from a Tor Exit node.



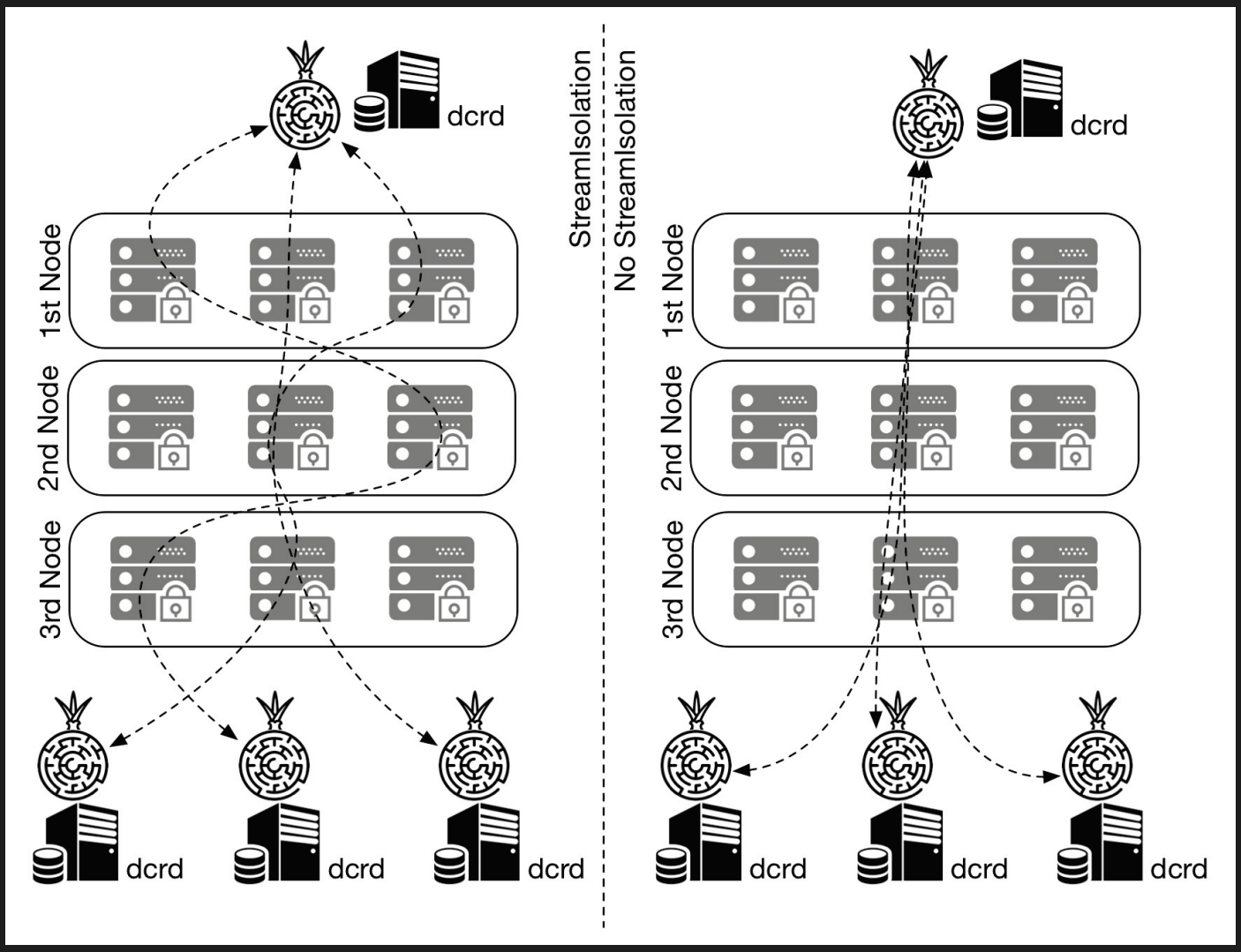
If an adversary somehow manages to compromise the Tor network too, they will only reveal the IP of a random public Wi-Fi that is not tied to your identity.

If an adversary somehow compromises your VM OS (with a malware or exploit for instance), they will be trapped within the internal Network of Whonix and should be unable to reveal the IP of the public Wi-Fi.

This solution however has one main drawback to consider: Interference with Tor Stream Isolation[320].

Stream isolation is a mitigation technique used to prevent some correlation attacks by having different Tor Circuits for each application. Here is an illustration to show what stream isolation is:

[320] Whonix Documentation, Stream Isolation https://www.whonix.org/wiki/Stream_Isolation [Archive.org]



(Illustration from Marcelo Martins, https://stakey.club/en/decred-via-tor-network/ [Archive.org])

VPN/Proxy over Tor falls on the right-side[321] meaning using a VPN/Proxy over Tor forces Tor to use one circuit for all activities instead of multiple circuits for each. This means that using a VPN/Proxy over Tor can somewhat reduce the effectiveness of Tor in some cases and should therefore be used only for some specific cases:

- When your destination service does not allow Tor Exit nodes.
- When you do not mind using a shared Tor circuit for various services. Like for instance for using various authenticated services.

You should however consider not using this method when your aim is just to browse random various unauthenticated websites as you will not benefit from Stream Isolation and this could make correlation attacks easier for an adversary between each of your sessions (see Your Anonymized Tor/VPN traffic).

More information at:

- https://www.whonix.org/wiki/Stream_Isolation [Archive org]
- https://tails.boum.org/contribute/design/stream_isolation/ [Archive org]
- https://www.whonix.org/wiki/Tunnels/Introduction#Comparison_Table [Archive.org]

Tor over VPN:

You might be wondering: Well, what about using Tor over VPN instead of VPN over Tor? Well, I would not necessarily it:

- Disadvantages

[321] Whonix Documentation, Tunnels Comparison Table, https://www.whonix.org/wiki/Tunnels/Introduction#Comparison_Table [Archive org]

    - Your VPN provider is just another ISP that will then know your origin IP and will be able to de-anonymize you if required. We do not trust them. I prefer a situation where your VPN provider does not know who you are. It does not add much in terms of anonymity.
    - This would result in you connecting to various services using the IP of a Tor Exit Node which are banned/flagged in many places. It does not help in terms of convenience.
- Advantages:
    - **The main advantage really is that if you are in a hostile environment where Tor access is impossible/dangerous/suspicious but VPN is okay.**
    - This method also does not break Tor Stream isolation.

Note, if you're having issues accessing the Tor Network due to blocking/censorship, you could try using Tor Bridges (see Tor Documentation https://2019.www.torproject.org/docs/bridges [Archive org] and Whonix Documentation https://www.whonix.org/wiki/Bridges [Archive org]).

It is also possible to consider **VPN over Tor over VPN (User > VPN > Tor > VPN > Internet)** using two cash/Monero paid VPNs instead. This means that you will connect the Host OS to a first VPN from your Public Wi-Fi, then Whonix will connect to Tor and finally your VM will connect to a second VPN over Tor over VPN (see https://www.whonix.org/wiki/Tunnels/Connecting_to_a_VPN_before_Tor [Archive.org]).

This will of course have a significant performance impact and might be quite slow but I think Tor is necessary somewhere for achieving reasonable anonymity.

Achieving this technically is easy within this route, you need two separate anonymous VPN accounts and must connect to the first VPN from the Host OS and follow the route.

Conclusion: Only do this if you think using Tor alone is risky/impossible but VPNs are okay. Or just because you can and so why not.

VPN only:
This route will not be explained nor recommended.

If you can use VPNs then you should be able to add a Tor layer over it. And if you can use Tor, then you can add an anonymous VPN over Tor to get the preferred solution.

Just using a VPN or even a VPN over VPN makes no sense as those can be traced back to you over time. One of the VPN providers will know your real origin IP (even if it is in a safe public space) and even if you add one over it, the second one will still know you were using that other first VPN service. This will only slightly delay your de-anonymization. Yes, it is an added layer … but it is a persistent centralized added layer and you can be de-anonymized over time. This is just chaining 3 ISPs that are all subject to lawful requests.

For more info, please see the following references:

- https://www.whonix.org/wiki/Comparison_Of_Tor_with_CGI_Proxies,_Proxy_Chains,_and_VPN_Services#Tor_and_VPN_Services_Comparison [Archive.org]
- https://www.whonix.org/wiki/Why_does_Whonix_use_Tor [Archive.org]
- https://www.researchgate.net/publication/324251041_Anonymity_communication_VPN_and_Tor_a_comparative_study [Archive.org]
- https://gist.github.com/joepie91/5a9909939e6ce7d09e29#file-vpn-md [Archive org]
- https://schub.wtf/blog/2019/04/08/very-precarious-narrative.html [Archive.org]

In the context of this guide, Tor is required somewhere to achieve reasonable and safe anonymity and you should use it if you can.

No VPN/Tor:
If you cannot use VPN nor Tor where you are, you probably are in a very hostile environment where surveillance and control is very high.

Just do not, it is not worth it and too risky IMHO. You can be de-anonymized almost instantly by any motivated adversary that could get to your physical location in a matter of minutes.

Do not forget to check back on Adversaries (threats) and Appendix S: Check your network for surveillance/censorship using OONI.

If you have absolutely no other option and still want to do something, see Appendix P: Accessing the internet as safely as possible when Tor/VPN is not an option **(at your own risk).**

Conclusion:

Connection Type	Anonymity	Ease of Access to online resources	Tor Stream isolation	Safer where Tor is suspicious/ dangerous	Speed	Cost	Recommended
Tor Alone	Good	Medium	Possible	No	Medium	Free	Yes
Tor over VPN	Good+	Medium	Possible	Yes	Medium	Around 50€/y	If needed (Tor inaccessible)
Tor over VPN over Tor	Best	Medium	Possible	Yes	Poor	Around 50€/y	Yes
VPN/Proxy over Tor	Good-	Good	Broken	No	Medium	Around 50€/y	If needed (convenience)
VPN/Proxy over Tor over VPN	Good-	Good	Broken	Yes	Poor	Around 100€/y	If needed (convenience and Tor inaccessible)
VPN/Proxy Alone	Bad	Good	N/A	Yes	Good	Around 50€/y	No, this is just non-sense.
No Tor and VPN	Bad	Unknown	N/A	No	Good	Around 100€ (Antenna)	No. At your own risk.

Unfortunately, using Tor alone will raise the suspicion of many destinations' platforms. You will face many hurdles (captchas, errors, difficulties signing-up) if you only use Tor. In addition, using Tor where you are could put you in trouble just for that. But Tor remains the best solution for anonymity and must be somewhere for anonymity.

- If your intent is to create persistent shared and authenticated identities on various services where access from Tor is hard, I recommend the **VPN over Tor** option (or VPN over Tor over VPN if needed). It might be a little less secure against correlation attacks due to breaking Tor Stream isolation but provides much better convenience in accessing online resources than just using Tor. It is an "acceptable" trade-off IMHP if you are careful enough with your identity.
- If your intent however is just to browse random services anonymously without creating specific shared identities, using tor friendly services; or if you do not want to accept that trade-off in the previous option. **Then I recommend using the Tor Only route to keep the full benefits of Stream Isolation (or Tor over VPN if you need to).**
- If cost is an issue, I recommend the Tor Only option if possible.
- If both Tor and VPN access are impossible or dangerous then you have no choice but to rely on Public wi-fis safely. See Appendix P: Accessing the internet as safely as possible when Tor and VPNs are not an option

For more information, you can also see the discussions here that could help decide yourself:

- Tor Project: https://gitlab.torproject.org/legacy/trac/-/wikis/doc/TorPlusVPN [Archive.org]
- Tails Documentation:
  - https://gitlab.tails.boum.org/tails/blueprints/-/wikis/vpn_support/ [Archive.org]
  - https://tails.boum.org/support/faq/index.en.html#index20h2 [Archive.org]
- Whonix Documentation (in this order):
  - https://www.whonix.org/wiki/Tunnels/Introduction [Archive.org]
  - https://www.whonix.org/wiki/Tunnels/Connecting_to_Tor_before_a_VPN [Archive.org]

    - https://www.whonix.org/wiki/Tunnels/Connecting_to_a_VPN_before_Tor [Archive.org]
- Some papers on the matter:
    - https://www.researchgate.net/publication/324251041_Anonymity_communication_VPN_and_Tor_a_comparative_study [Archive.org]

Get an anonymous VPN/Proxy:

Skip this step if you want to use Tor only or VPN is not an option.

See Appendix O: Get an anonymous VPN/Proxy

Installation:

We will follow the instructions from their own guide https://www.qubes-os.org/doc/installation-guide/ [Archive.org]:

Secure Boot is not supported as per their FAQ: https://www.qubes-os.org/faq/#is-secure-boot-supported [Archive.org] so it should be disabled in the BIOS/UEFI settings.

- Download the latest Qubes OS installation ISO according to their hardware compatibility list.
- Prepare an USB key with the Qubes OS ISO file
- Install Qubes OS according to the installation guide:
    - **If you want to use Tor or VPN over Tor: Check the "Enabling system and template updates over the Tor anonymity network using Whonix" during the last step. This will force all Qubes OS updates to go through Tor. While this will significantly reduce your update speed, it will increase your anonymity from the start.** (If you are having issues connecting to Tor due to censorship or blocking, consider using Tor Bridges as recommended earlier. Just follow the tutorial provided here: https://www.whonix.org/wiki/Bridges [Archive org])
    - If you want to use Tor over VPN or cannot use any of those, leave it unchecked.
- If you cannot use Tor at all, there is also no point in installing Whonix. So, you should disable Whonix installation within the Software Selection Menu.

Lid Closure Behavior:

Unfortunately, Qubes OS does not support hibernation[322] which is IMHO an issue regarding cold-boot attacks. To mitigate those, I highly recommend that you configure Qubes OS to shut down on any power action (power button, lid closure). You can do set this from the XFCE Power Manager. Do not use the sleep features.

Connect to a Public Wi-Fi:

Remember this should be done from a safe place (see Find some safe places with decent public Wi-Fi and Appendix Q: Using long range Antenna to connect to Public Wi-Fis from a safe distance).

- In the upper right corner, Left click the network icon and note the Wi-Fi SSID you want to connect to
- Now right click the network icon and select Edit Connections
- Add one using the + sign
- Select Wi-Fi
- Enter the SSID of the desired network you noted before (if required)
- Select Cloned Mac Address
- Select Random to randomize your Mac Address
    - **Warning: This setting should work in most cases but can be unreliable on some network adapters. Please refer to this documentation if you want to be sure: https://github.com/Qubes-Community/Contents/blob/master/docs/privacy/anonymizing-your-mac-address.md** [Archive.org]
- Save
- Now again Left click the connection account and connect to the desired Wi-Fi
- If this is an Open Wi-Fi requiring registration: You will have to start a browser to register
    - After you are connected, Start a Disposable Fedora Firefox Browser

[322] Qubes OS Issues, Simulate Hibernation / Suspend-To-Disk #2414 https://github.com/QubesOS/qubes-issues/issues/2414 [Archive org]

- Go into the upper left Menu
- Select Disposable, Fedora, Firefox
- Open Firefox and register (anonymously) into the Wi-Fi

Update Qubes OS:

After you are connected to a Wi-Fi you need to update Qubes OS and Whonix. It is important that you keep Qubes OS always updated before conducting any sensitive activities. Especially your Browser VMs. Normally, Qubes OS will warn you about updates in the upper right corner with a gear icon. As this might take a while in this case due to using Tor, you can force the process by doing the following:

- Click the upper left Applications icon
- Select System Tools
- Select Qubes Update and Launch it
- Check the "Enable updates for qubes without known available updates"
- Select all the Qubes
- Click Next and update
- If you checked the Tor option during install, wait patiently as this might take a while over Tor

Hardening Qubes OS:

Disclaimer: This section is under construction and will be worked on heavily in the next releases. This section is for more advanced users.

Application Sandboxing:

While Qubes OS is already sandboxing everything by design, it is also useful to consider sandboxing apps themselves using AppArmor or SELinux.

AppArmor:

"AppArmor is a Mandatory Access Control framework. When enabled, AppArmor confines programs according to a set of rules that specify what files a given program can access. This proactive approach helps protect the system against both known and unknown vulnerabilities" (Debian.org).

Basically, AppArmor[323] is an application sandboxing system. By default, it is not enabled but supported by Qubes OS.

- About the Fedora VMs:
  - Fedora does not really use AppArmor but rather SELinux so see next section for that.
- About the Debian VMs:
  - Head out and read https://wiki.debian.org/AppArmor [Archive.org]
- About any other Linux VM:
  - Head out and read:
    - https://wiki.archlinux.org/title/AppArmor [Archive.org]
    - https://wiki.debian.org/AppArmor [Archive.org]
- About the Whonix VMs, you should consider enabling it and using it, especially on the Whonix VMs of Qubes OS:
  - First you should head out and read https://www.whonix.org/wiki/AppArmor [Archive.org]
  - Secondly you should head out again and read https://www.whonix.org/wiki/Qubes/AppArmor [Archive org]

SELinux:

SELinux[324] is similar to AppArmor. The differences between SELinux and AppArmor are technical details we will not get into.

Here is a good explanation of what it is: https://www.youtube.com/watch?v=_WOKRaM-HI4 [Invidious]

---

[323] Wikipedia, AppArmor https://en.wikipedia.org/wiki/AppArmor [Wikiless] [Archive.org]

[324] Wikipedia, SELinux https://en.wikipedia.org/wiki/Security-Enhanced_Linux [Wikiless] [Archive.org]

In this guide and the context of Qubes OS, it is important to mention it as it is the recommended method by Fedora which is one of the default systems on Qubes OS.

So, head out and read https://docs.fedoraproject.org/en-US/quick-docs/getting-started-with-selinux/ [Archive.org]

You could make use of SELinux on your Fedora Templates. But this is up to you. Again, this is for advanced users.

Setup the VPN ProxyVM:

Skip this step if you do not want to use a VPN and just use Tor only or if VPN is not an option either.

This tutorial should also work with any OpenVPN provider (Mullvad, IVPN or ProtonVPN for instance).

This is based on the tutorial provided by Qubes OS themselves (https://github.com/Qubes-Community/Contents/blob/master/docs/configuration/vpn.md [Archive.org]). If you are familiar with this process, you can follow their tutorial. Here is mine:

Create the ProxyVM:

- Click the Applications icon (upper left corner)
- Click Create Qubes VM
- Name and label as you wish: I suggest "VPNGatewayVM"
- Select Type: Standalone Qube copied from a template
- Select Template: debian-10
- Select Networking:
    - Select sys-whonix if you want to do VPN over Tor / Tor only (recommended)
    - Select sys-firewall if you want to do Tor over VPN / No Tor or VPN / Just VPN
- Advanced: Check provides network
- Check "Start qube automatically on boot"
- Create the VM
- Test your Connectivity:
    - If you are going for VPN over Tor, Test the VM connectivity to Tor by launching a Browser within the ProxyVM and going to https://check.torproject.org [Archive.org] (It should say you are connected to Tor)
    - If you are going for Tor over VPN, Test the VM connectivity to the internet by launching a Browser within the ProxyVM and access any website.

Download the VPN configuration from your cash/Monero paid VPN provider:

If you can use Tor:

Using Tor browser (be careful not to use any Clearnet Browser for this), download the necessary OpenVPN configuration files for Linux from your VPN provider.

This can be done by using the Qubes OS integrated Tor Browser by accessing the Applications icon (upper left corner) and selecting the Disposable Tor Browser application.

If you cannot use Tor:

Launch a browser from a DisposableVM and download the necessary OpenVPN configuration files for Linux from your VPN provider. See Appendix P: Accessing the internet as safely as possible when Tor and VPNs are not an option.

When you are done downloading the configuration files within the Disposable Browser (usually a zip file), copy them to your ProxyVM VPN Gateway machine (using right click on the file and send to another AppVM).

Configure the ProxyVM:

Skip this step if you are not going to use a VPN

- Click the upper left corner
- Select the VPN VM you just created
- Open the Files of the VPN VM
- Go into "Qubesincoming" > dispXXXX (This was your Disposable Browser VM)

- Double Click your downloaded zip file containing your OpenVPN configuration files to unzip it
- Now select the VPN VM again and start a terminal
- Install OpenVPN with the following command ```sudo apt-get install openvpn```
- Copy all the OpenVPN configuration files provided by your VPN provider in /etc/openvpn/
- For all the OpenVPN configuration files (for each location):
    - Edit each file using ```sudo nano configfile``` (do not forget sudo to edit file within /etc)
    - Change the protocol from "udp" to "tcp" (Tor does not support UDP)
    - Change the port to a supported (by your VPN provider) TCP port (like 80 or 443)
    - Save and exit each file
- Edit the OpenVPN config file (/etc/default/openvpn) by typing ```sudo nano /etc/default/openvpn``` (because I do not like vi editor)
    - Change ```#AUTOSTART="all"``` to ```AUTOSTART="all"``` (in other words, remove the "#")
    - Save and Exit
- Edit the Qubes firewall rules file (/rw/config/qubes-firewall-user-script) by typing "sudo nano /rw/config/qubes-firewall-user-script"
    - Add the following lines (without the quotes and remarks in parentheses)
        - ```virtualif=10.137.0.17```

          (This is the IP of the ProxyVM, this is not dynamic and you might need to change it at reboot)

        - ```vpndns1=10.8.0.1```

          (This is the first DNS server of your VPN provider; it should not change)

        - ```vpndns2=10.14.0.1```

          (This is the second DNS server of your VPN provider; it should not change)

        - ```iptables -F OUTPUT```
        - ```iptables -I FORWARD -o eth0 -j DROP```
        - ```iptables -I FORWARD -i eth0 -j DROP```
        - ```ip6tables -I FORWARD -o eth0 -j DROP```
        - ```ip6tables -I FORWARD -i eth0 -j DROP```

          (These will block outbound traffic when the VPN is down, it is a kill switch, more information here https://linuxconfig.org/how-to-create-a-vpn-killswitch-using-iptables-on-linux [Archive.org])

        - ```iptables -A OUTPUT -d 10.8.0.1 -j ACCEPT```
        - ```iptables -A OUTPUT -d 10.14.0.1 -j ACCEPT```

          (These will allow DNS request to your VPN provider DNS to resolve the name of the VPN servers in the OpenVPN configuration files)

        - ```iptables -F PR-QBS -t nat```
        - ```iptables -A PR-QBS -t nat -d $virtualif -p udp --dport 53 -j DNAT --to $vpndns1```
        - ```iptables -A PR-QBS -t nat -d $virtualif -p tcp --dport 53 -j DNAT --to $vpndns1```
        - ```iptables -A PR-QBS -t nat -d $virtualif -p udp --dport 53 -j DNAT --to $vpndns2```
        - ```iptables -A PR-QBS -t nat -d $virtualif -p tcp --dport 53 -j DNAT --to $vpndns2```

          (These will redirect all DNS requests from the ProxyVM to the VPN provider DNS servers)

- Restart the ProxyVM by typing "sudo reboot"
- Test the ProxyVM VPN connectivity by starting a Browser within it and going to your VPN provider test page. It should now say you are connected to a VPN:
    - Mullvad: https://mullvad.net/en/check/ [Archive.org]
    - IVPN: https://www.ivpn.net/ [Archive.org] (check the top banner)
    - ProtonVPN: Follow their instructions here https://protonvpn.com/support/vpn-ip-change/ [Archive.org]

VPN over Tor:

Setup a disposable Browser Qube for VPN over Tor use:

- Within the Applications Menu (upper left corner), Select the Disposable Fedora VM
- Go into Qube Settings
- Click Clone qube and name it (like "VPNoverTor")
- Again, within the Application Menu, Select the Clone you just created
- Go into Qube Settings
- Change the Networking to your ProxyVPN created earlier
- Click OK
- Start a Browser within the Whonix Workstation
- Check that you have VPN connectivity and it should work

You should now have a Disposable Browser VM that works with your cash/Monero paid VPN over Tor.

Tor Over VPN:

Reconfigure your Whonix Gateway VM to use your ProxyVM as NetVM instead of sys-firewall.

- Within the Applications Menu (upper left corner), Select the sys-whonix VM.
- Go into Qube Settings
- Change the Networking NetVM to your ProxyVPN created earlier instead of sys-firewall
- Click OK
- Create a Whonix Workstation Disposable VM (follow this tutorial https://www.whonix.org/wiki/Qubes/DisposableVM [Archive.org])
- Launch a browser from the VM and Check that you have VPN connectivity and it should work.

Alternatively, you can also create any other type of disposable VM (but probably less secure than the Whonix one):

- Within the Applications Menu (upper left corner), Select the Disposable Fedora VM
- Go into Qube Settings
- Click Clone qube and name it (like "TorOverVPN")
- Again, within the Application Menu, Select the Clone you just created
- Go into Qube Settings
- Change the Networking to your sys-whonix created earlier
- Click OK
- Start a Browser within the VM
- Check that you have VPN connectivity and it should work

You should now have a Disposable Browser VM that works with Tor over a cash/Monero paid VPN.

Any other combination? (VPN over Tor over VPN for instance)

By now you should understand how easy it is to route traffic from one VM to the other with Qubes.

You can create several ProxyVMs for VPN accesses and keep the Whonix one for Tor. You just need to change the NetVM settings of the various VMs to change the layout.

You could have:

- One VPN ProxyVM for the base Qubes OS connection
- Use the sys-whonix VM (Whonix Gateway) getting its network from the first ProxyVM
- A second VPN ProxyVM getting network from sys-whonix
- Disposable VMs getting their NetVM from the second ProxyVM

This would result in User > VPN > Tor > VPN > Internet (VPN over Tor over VPN). Experiment for yourself. Qubes OS is great for these things.

Setup a safe Browser within Qubes OS (optional but recommended):

Fedora Disposable VM:

This time, I will recommend the Chromium based Brave browser instead of Tor Browser

See why here: Appendix V: What browser to use in your Guest VM/Disposable VM

Within the Applications Menu (upper left), Select the Fedora-30 template

- Go into Qube Settings
- Clone the VM and name it "fedora-30-brave" (this VM template will have Brave)
- Again, go into the Applications Menu and select the clone you just created
- Go into Qube Settings
- Change its network to the ProxyVPN and Apply
- Launch a terminal from the VM

Apply the instructions from https://brave.com/linux/ [Archive org] (Fedora 28+ section) and run the following commands:

- ```sudo dnf install dnf-plugins-core```
- ```sudo dnf config-manager --add-repo https://brave-browser-rpm-release.s3.brave.com/x86_64/```
- ```sudo rpm --import https://brave-browser-rpm-release.s3.brave.com/brave-core.asc```
- ```sudo dnf install brave-browser```

Whonix Disposable VM:

Edit the Whonix Disposable VM template and follow instructions here
https://www.whonix.org/wiki/Install_Software [Archive.org]

Setup an Android VM:

Because sometimes you want to run mobile Apps anonymously too. You can also set-up an Android VM for this purpose. As in other cases, ideally this VM will also be sitting behind the Whonix Gateway for Tor network connectivity. But this can also be set-up as VPN over Tor over VPN.

Since the x86 Android does not work "well" with Qubes OS. I will instead recommend using AnBox.io which works "well enough" with Qubes OS.

If you can use Tor (natively or over a VPN):

Later in the Qubes settings during creation:

- Select Networking
- Change to sys-Whonix to put it behind the Whonix Gateway (over Tor).

If you cannot use Tor:

Just use the tutorials as is. See Appendix P: Accessing the internet as safely as possible when Tor and VPNs are not an option.

Installation:

Basically, follow the tutorial here:

- Click the Applications icon (upper left corner)
- Click Create Qubes VM
- Name and label as you wish: I suggest "Android Box"
- Select Type: Standalone Qube copied from a template
- Select Template: debian-10
- Select Networking:
  - Select sys-whonix if you want to do VPN over Tor / Tor only (recommended)
  - Select sys-firewall if you want to do Tor over VPN / No Tor or VPN / Just VPN
- Start the Qube and open a Terminal

Now you will have to follow the instructions from here: https://github.com/anbox/anbox-modules [Archive.org]

- Start by closing the AnBox Modules repository by running:
  - ```git clone https://github.com/anbox/anbox-modules.git```
  - Go into the clone directory
  - Run ```./INSTALL.sh``` (or follow the manual instructions on the tutorial)
- Reboot the machine
- Open a new terminal
- Install Snap by running:
  - ```sudo apt install snapd```

Now we will follow their other tutorial from here: https://github.com/anbox/anbox/blob/master/docs/install.md [Archive org]

- Install AnBox by running:
  - ```snap install --devmode --beta anbox```
- To update AnBox later, run:
  - ```snap refresh --beta --devmode anbox```
- Reboot the machine
- Open a terminal again and start the emulator by running:
  - ```anbox.appmgr```

This should pop-up an Android interface. Sometimes it will crash and you might have to run it twice to make it work.

If you want to install apps on this emulator:

- Install ADB by running:
  - ```sudo apt install android-tools-adb```
- First start Anbox (run ```anbox.appmgr```)
- Grab the APK of any app you want to install
- Now install any APK by running:
  - ```adb install my-app.apk```

That's it, you should now have an Android Qube over Tor (or anything else) capable of running pretty much any App you can sideload with ADB. This is, for now and IMHO, the easiest way to get Android emulation on Qubes OS.

KeePassXC:

You will need something to store your data (logins/passwords, identities and TOTP[325] information).

For this purpose, I strongly recommend KeePassXC because of their integrated TOTP feature. This is the ability to create entries for 2FA[326] authentication with the authenticator feature.

In the context of Qubes OS you should probably store your sensitive information within the Domain-vault qube.

- First click the Applications icon (upper left) and select the Domain: Vault qube.
- Click Qubes Settings
- Temporarily enable network by changing the network to your VPN ProxyVM you created earlier
- Open a terminal within the Domain: Vault qube
- Type: ```sudo dnf install keepassxc``` and wait for it to install
- Close the terminal and disable network by changing back the network to (none)
- Go back into the Domain: Vault Qube Settings and into the Applications tab
- Click Refresh
- Add KeePassXC to the Selected tab
- Launch KeePassXC within the Domain: Vault qube

---

[325] Wikipedia, TOTP https://en.wikipedia.org/wiki/Time-based_One-time_Password_algorithm [Wikiless] [Archive.org]

[326] Wikipedia, Multi-Factor Authentication https://en.wikipedia.org/wiki/Multi-factor_authentication [Wikiless] [Archive.org]

You are done and can now skip the rest to go to the "Creating your anonymous online identities" part.

Creating your anonymous online identities:

Understanding the methods used to prevent anonymity and verify identity:

Captchas:

(Illustration by xkcd.com, licensed under CC BY-NC 2.5)

Captcha[327] stands for "Completely Automated Public Turing test to tell Computers and Humans Apart" are Turing tests[328] puzzles you need to complete before accessing a form/website. You will mostly encounter those provided by Google (reCaptcha service[329]) and Cloudflare (hCaptcha[330]). hCaptcha is used on 15% of the internet by their own metrics[331].

They are designed to separate bots from humans but are also clearly used to deter anonymous and private users from accessing services.

If you frequently use VPNs or Tor, you will quickly encounter many captchas everywhere[332]. Quite often when using Tor, even if you succeed in solving all the puzzles (sometimes dozens in a row), you will still be denied after solving the puzzles.

See https://gitlab.torproject.org/legacy/trac/-/wikis/org/doc/ListOfServicesBlockingTor [Archive.org]

---

[327] Wikipedia, Captcha https://en.wikipedia.org/wiki/CAPTCHA [Wikiless] [Archive.org]

[328] Wikipedia, Turing Test https://en.wikipedia.org/wiki/Turing_test [Wikiless] [Archive.org]

[329] Google reCaptcha https://www.google.com/recaptcha/about/ [Archive.org]

[330] hCaptcha https://www.hcaptcha.com/ [Archive.org]

[331] hCaptcha, hCaptcha Is Now the Largest Independent CAPTCHA Service, Runs on 15% Of The Internet https://www.hcaptcha.com/post/hcaptcha-now-the-largest-independent-captcha-service [Archive.org]

[332] Nearcyan.com, You (probably) don't need ReCAPTCHA https://nearcyan.com/you-probably-dont-need-recaptcha/ [Archive.org]

While most people think those puzzles are only about solving a little puzzle, it is important to understand that it is much more complex and that modern Captchas uses advanced machine learning and risk analysis algorithms to check if you are human[333]:

- They check your browser, cookies and browsing history using Browser fingerprinting[334].
- They track your cursor movements (speed, accuracy) and use algorithms to determine if it is "human/organic".
- They track your behavior before/during/after the tests to ensure you are "human"[335].

It is also very likely that those platforms could already reliably identify you based on the unique way you interact with those puzzles. This could work despite obfuscation of your IP address / Browser and clearing all cookies.

You will often experience several in a row (sometimes endlessly[336]) and sometimes very difficult ones involving reading undecipherable characters or identifying various objects on endless pictures sets. You will also have more captchas if you use an ad blocking system (uBlock for example) or if your account was flagged for any reason for using VPNs or Tor previously.

You will also have (in my experience) more Captchas (Google's reCaptcha) if you do not use a Chromium based browser. But this can be mitigated by using Chromium based browsers such as Brave or Ungoogled-Chromium. There is also a Browser extension called Buster that could help you those https://github.com/dessant/buster [Archive org].

As for Cloudflare (hCaptcha), you could also use their Accessibility solution here (https://www.hcaptcha.com/accessibility [Archive.org]) which would allow you to sign-up (with your anonymous identity created later) and set a cookie within your Browser that would allow you to bypass their captchas. Another solution to mitigate hCaptcha would be to use their own solution called "Privacy Pass"[337] https://privacypass.github.io/ [Archive org] in the form of a Browser extension you could install in your VM Browser.

You should therefore deal with those carefully and force yourself to alter the way you are solving them (speed/movement/accuracy/…) as to prevent "Captcha Fingerprinting".

Fortunately, as far as I am aware, these are not yet officially/publicly used to de-anonymize users for third parties.

Phone verification:

Phone verification is advertised by most platforms to verify you are human. But do not be fooled, the main reason for phone verification is not only to check if you are human but also to be able to de-anonymize you if needed.

Most platforms (including the privacy-oriented ones such as Signal/Telegram/ProtonMail will require a phone number to register and most countries now make it mandatory to submit a proof of ID to register[338].

E-Mail verification:

E-Mail verification is what used to be enough but is not anymore in most cases. What is important to know is that open e-mail providers (disposable e-mail providers for instance) are flagged as much as open proxies (like Tor).

Most platforms will not allow you to register using an "anonymous" or disposable e-mail. As they will not allow you to register using an IP address from the Tor network.

---

[333] ArsTechnica, "Google's reCAPTCHA turns "invisible," will separate bots from people without challenges" https://arstechnica.com/gadgets/2017/03/googles-recaptcha-announces-invisible-background-captchas/ [Archive.org]

[334] BlackHat Asia 2016, "I'm not a human: Breaking the Google reCAPTCHA", https://www.blackhat.com/docs/asia-16/materials/asia-16-Sivakorn-Im-Not-a-Human-Breaking-the-Google-reCAPTCHA-wp.pdf [Archive.org]

[335] Google Blog https://security.googleblog.com/2014/12/are-you-robot-introducing-no-captcha.html [Archive.org]

[336] Tor Project Community, Cloudflare Captcha Monitoring https://community.torproject.org/gsoc/cloudflare-captcha-monitoring/ [Archive.org]

[337] Cloudflare Blog, Cloudflare supports Privacy Pass https://blog.cloudflare.com/cloudflare-supports-privacy-pass/ [Archive.org]

[338] Privacy International, Timeline of SIM Card Registration Laws https://privacyinternational.org/long-read/3018/timeline-sim-card-registration-laws [Archive.org]

The key thing to this is that it is becoming increasingly difficult to sign-up for a free e-mail account anywhere without providing (you guessed it) … a mobile phone number. That same mobile phone number that can be used conveniently to track you down in most places.

If you want to avoid communicating your anonymous e-mail address to various parties, you could consider using some e-mail aliasing services such as:

- https://anonaddy.com/
- https://simplelogin.io/

These services will allow to create aliases for your anonymous e-mail (on ProtonMail or example) and could increase your general privacy if you do not want to disclose that e-mail for any purpose. They are both recommended by privacytools.Io

It is possible that those services (ProtonMail for instance) might require you to provide an e-mail address for registration. In that case, I would recommend you create an e-mail address from these providers:

- Disroot https://disroot.org
- RiseUp https://riseup.net
- Autistici https://autistici.org

Keep in mind that those do not provide a zero-access design where only you can access your e-mail.

User details checking:

Obviously, Reddit does not do this (yet) but Facebook most likely does and will look for "suspicious" things in your details (which could include face recognition).

Some examples:

- IP address from a country different than your profile country?
- Age in the profile not matching the picture age?
- Ethnicity in the profile not matching the picture ethnicity?
- Language not matching the country language?
- Unknown in anyone else contacts? (Meaning nobody else knows you?)
- Locking down privacy settings after signing-up?
- Name that does not match the correct ethnicity/language/country?

Proof of ID verification:

The deal-breaker in most cases. As far as I know, only Facebook and LinkedIn (outside of financial services) have requested such verifications which involves sending pictures of some form of identification (passport, national ID card, driver license …). The only way to do this would involve creating fake official documents (forgery) using some decent Photoshop skills and this might be illegal in most places.

Therefore, this is a line I am not going to help you cross within this guide. Some services are offering such services online but I think they most likely are *bad actors* and are most likely overstepping their boundaries.

In many countries, only law enforcement, some very specific processes (such as GDPR request) and some well-regulated financial services are authorized to request a proof of identification. So, the legality of asking such documents is debatable and I think such platforms should not be allowed to require those.

In few countries (like Germany), this practice is illegal and online platforms such as Facebook or LinkedIn are legally bound to allow you use a pseudonym and remain anonymous.

IP Filters:

As stated previously in this guide, many platforms will apply filters on the IPs of the users. Tor exit nodes are publicly listed and VPN exit servers are "well known". There are many commercial and free services providing the ability to block those IPs with ease (hi Cloudflare).

Many platforms' operators and administrators do not want traffic from these IPs as they often drive a lot of unlawful/malicious/unprofitable traffic to their platforms. Usually using the same excuses:

- Unlawful because "Think of the children" or "Terrorists".
- Malicious because "Russian trolls".
- Unprofitable because "Well it's noise in the data we sell to advertisers" (AdSense, Facebook Ads …). Yet we still pay traffic for them so let us just deny them all instead.

Fortunately, those systems are not "perfect' and you will (still) be able to get around those restrictions by switching identities (in the case of Tor) and looking trying to access the website each time until you find an Exit Node that is not blacklisted (yet).

Sometimes some platforms will allow you to log-in with a Tor IP but not sign-up (See https://gitlab.torproject.org/legacy/trac/-/wikis/org/doc/ListOfServicesBlockingTor [Archive org]). Obviously, those platforms will keep a convenient permanent log of the IP you used during sign-up. And some will keep such logs indefinitely including all the IPs you used to logging in (hi Facebook).

The tolerance is much higher with VPNs as they are not considered "open proxies" but that will not stop many platforms from making them hard to use by forcing increasingly difficult captchas on most VPN users.

For this reason, this guide recommends the use of VPN over Tor (and not Tor over VPN).

Browser and Device Fingerprinting:

Browser and Device[339] Fingerprinting are usually integrated into the Captcha services but also in other various services.

Many platforms (like Google[340]) will check your browser for various capabilities and settings and block Browsers they do not like. This is one of the reasons I recommend using Chromium based Browsers such as Brave Browser over Tor Browser within this VM.

Here are some of the things they check within recent browsers:

- User Agent: This is your Browser name and Version.
- HTTP_ACCEPT Headers: This is the type of content your Browser can handle.
- Time Zone and Time Zone Offset: Your time zone.
- Screen Size and Color Depth: The resolution of your screen.
- System Fonts: The typing fonts installed on your system.
- Cookies support: If your Browser supports cookies or not.
- Hash of Canvas fingerprint and Hash of WebGL fingerprint: These are generated unique IDs based on your graphic rendering capabilities.
- WebGL Vendor & Renderer: Name of your Video card
- Do-Not-Track enabled or not: Well yes, they can use your DNT information to track you
- Language: The language of your Browser
- Platform: The Operating System you are using
- Touch Support: If your system supports touch (such as a phone/tablet or touchscreen enabled laptop)
- Ad Blocking use: If your browser block ads
- AudioContext fingerprint: Like the Canvas and WebGL fingerprints these will fingerprint your audio capabilities.
- CPU: What kind of CPU you are using and how many of them
- Memory: How much memory you have in your System
- Browser Permissions: Is your browser allowing some things like geolocation or microphone/webcam access.

---

[339] Wikipedia, Device Fingerprinting https://en.wikipedia.org/wiki/Device_fingerprint [Wikiless] [Archive org]

[340] Developers Google Blog,
Guidance to developers affected by our effort to block less secure browsers and applications
https://developers.googleblog.com/2020/08/guidance-for-our-effort-to-block-less-secure-browser-and-apps.html [Archive.org]

- …

Here are two services you can use to check your browser Fingerprinting:

- https://coveryourtracks.eff.org/
- https://amiunique.org
- https://browserleaks.com/

Chances are you will find your browser fingerprint unique no matter what you do.

Human interaction:

Some platforms will add this as a bonus step and require you to have an actual human interaction with a customer care representative. Usually by e-mail but sometimes by chat/phone. They will want to verify that you exist by asking you to reply to an e-mail/chat/phone call.

It is annoying but very easy to deal with in our case. We are not making bots. This guide is for humans making human accounts.

User Moderation:

Many platforms will delegate and rely on their own users to moderate the others and their content. These are the "report" features that you will find on most platforms.

Getting reported thousands of times does not matter when you are Donald Trump or Kim Kardashian but if you as a sole "friendless" anonymous user gets reported even once, you might get suspended/flagged/banned instantly.

Behavioral Analysis:

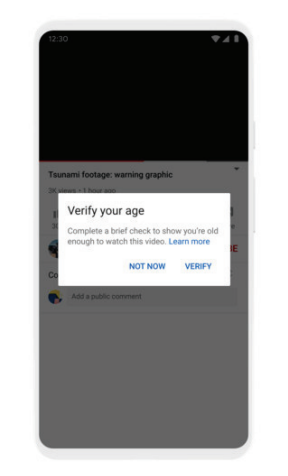
See Your Digital Fingerprint, Footprint, and Online Behavior.

Financial transactions:

Simple and efficient, some platforms will require than you perform financial transaction to verify your account sometimes under the pretext of verifying your age. This could be a credit card verification or a very small amount bank wire. Some will accept a donation in a main crypto like Bitcoin or Ethereum.

While this might seem innocent, this is obviously an ID verification and de-anonymization method. This is just indirectly relying on third party financial KYC[213] regulations.

This is for instance now the case on YouTube for some European Users[341] but also used by services like Amazon that requires a valid payment method for creating an account.



Sign-in with some platform:

Why do this user verification ourselves when we can just ask others to deal with it?

[341] Google Help, Access age-restricted content & features https://support.google.com/accounts/answer/10071085 [Archive.org]

You will notice this and you probably already encountered this. Some apps/platforms will ask/require you to sign-in with a well-known and well-used reputable platform instead of their own system (Sign-in with Google/Facebook/Apple/Twitter).

This option is often presented as the "default one", hiding away the "Sign-in with e-mail and password" with clever Dark Patterns[342] and unfortunately sometimes required.

This method will delegate the verification process on those platforms instead assuming that you will not be able to create an anonymous Google/Facebook/Apple/Twitter account with ease.

Fortunately, it is still possible to this day do create those.

Live Face recognition and biometrics (again):

This is a common method used on some Crypto trading platforms and some dating Apps.

Some platforms/apps will require you to take a live picture of yourself either doing something (a wink, holding an arm up …) or showing a custom piece of information (a hand written text, a passport or ID) within the picture. Sometimes the platform/app will require several pictures to increase their certainty.

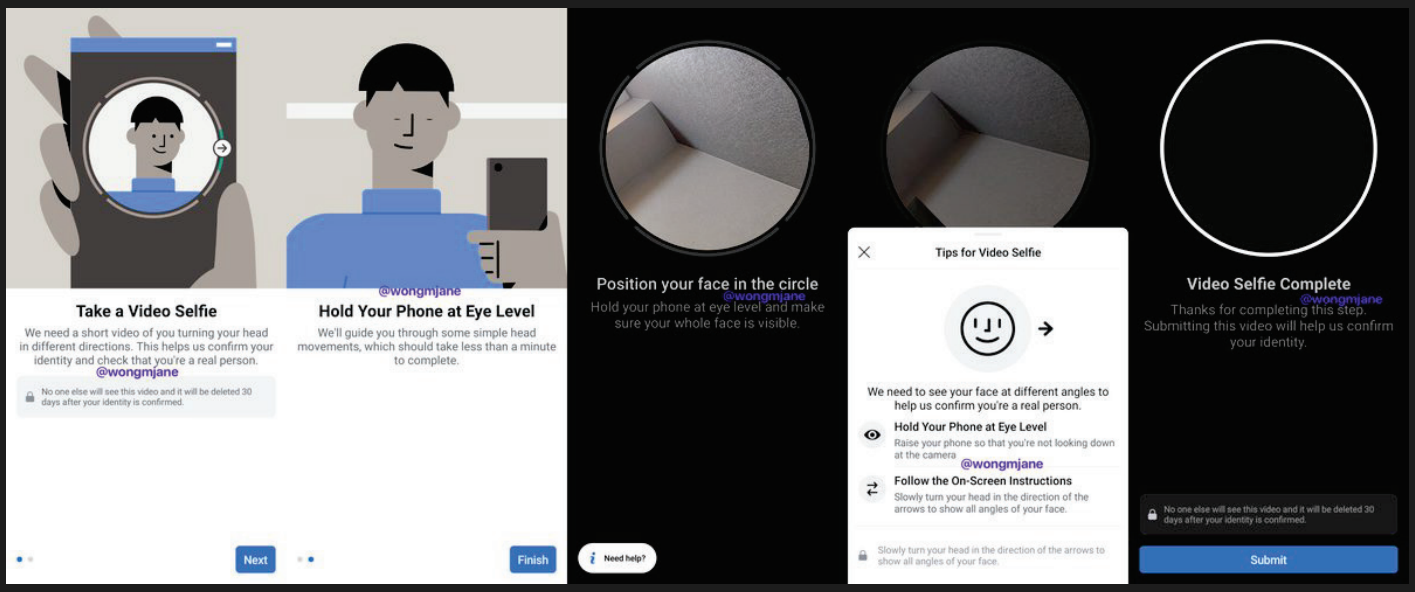
This guide will not cover this one (yet) as it is mainly used on financial platforms (that will be able to identify you with other means anyway) and some dating apps like Tinder[343]. Unfortunately, this method is now also sometimes being used on Facebook[344] and Instagram as part of their verification methods (tho I did not face it yet so far).

---

[342] Wikipedia, Dark Pattern https://en.wikipedia.org/wiki/Dark_pattern [Wikiless] [Archive.org]

[343] The Verge, Tinder will give you a verified blue check mark if you pass its catfishing test https://www.theverge.com/2020/1/23/21077423/tinder-photo-verification-blue-checkmark-safety-center-launch-noonlight [Archive org]

[344] DigitalInformationWorld, Facebook will now require you to Create a Video Selfie for Identity Verification https://www.digitalinformationworld.com/2020/03/facebook-is-now-demanding-some-users-to-create-a-video-selfie-for-identity-verification.html [Archive.org]



In some cases, these verifications must be done from your Smartphone and with an "in-app" camera to prevent you from sending a previously saved (edited) image.

Recently even platforms such as PornHub decided to implement similar measures in the future[345].

This verification is very hard to defeat but possible. A method to possibly defeat those would be to use "deep fake" technology software such as the open-source FaceSwap https://github.com/deepfakes/faceswap [Archive.org] to generate the required verification pictures using a randomly computer-generated face that would be swapped over the picture of a complicit model (or a stock photo).

Unfortunately, some apps require direct access to a smartphone camera to process the verification. In that case we will need to find a way to do such "face swaps" on the fly using a filter and another way to feed this into the camera used by the app.

Manual reviews:

These can be triggered by any of the above and just means someone (usually specialized employees) will review your profile manually and decide if it is real or not based on their subjective opinion.

Some countries have even developed hotlines where you can report any subversive content[346].

Pros: Usually that verdict is "final" and you will probably avoid further issues if you are good.

Cons: Usually that verdict is "final" and you will probably be banned without any appeal possibility if you are not good. Sometimes those reviews end up in the platform just ghosting you and cancel you without any reason whatsoever. Any appeal will be left unanswered, ignored, or will generate some random dark pattern bug when trying to appeal that specific identity (this happens on Instagram for instance where if your account gets "suspended" obviously by some manual review, trying to complete the appeal form will just throw an error and tell you to try again later (I have been trying this same appeal for that identity for the past 6 months at least).

Getting Online:

Now that you have a basic understanding of all the ways you can be de-anonymized, tracked and verified. Let us get started at evading these while remaining anonymous. Remember:

- You cannot trust ISPs
- You cannot trust VPS providers
- You cannot trust public Wi-Fi providers

---

[345] Vice.com, PornHub Announces 'Biometric Technology' to Verify Users https://www.vice.com/en/article/m7a4eq/pornhub-new-verification-policy-biometric-id [Archive.org]

[346] Variety, China Launches Hotline to Report Online Comments That 'Distort' History or 'Deny' Its Cultural Excellence https://variety.com/2021/digital/news/china-censorship-hotline-historical-nihilism-1234950554/ [Archive.org]

- You cannot trust Mobile Network providers
- You cannot trust VPN providers
- You cannot trust any Online Platform
- You cannot trust Tor
- You cannot trust your Operating systems (especially Android and Windows).
- You cannot trust your Laptop
- You cannot trust your Smartphone (especially Android).
- You cannot trust your Smart devices
- Above all, you cannot trust people.

So what? Well instead of not trusting anyone or anything, I would advise to **"Trust but verify"**[347] (or alternatively "Never trust, always verify" if you are more hardcore about it and want to apply Zero-Trust Security[348]) instead.

Do not start this process unless:

- **You consulted your local law for compliance and the legality of your actions.**
- **You are aware of your threat model.**
- **You are in a safe place with a public Wi-Fi without your smartphone or any other smart device on you. And preferably in a place without CCTV filming you (remember Find some safe places with decent public Wi-Fi and Appendix Q: Using long range Antenna to connect to Public Wi-Fis from a safe distance)**
- **You are fully done and preparing one of the routes.**
- **Again, it is crucially important to understand that you will be unable to create most accounts without a valid phone number. Therefore, most of your anonymity on mainstream platforms depends on the anonymity of your online phone number and/or the burner phone with its pre-paid SIM card (if you use one). If your phone number is not anonymous or your burner phone can be traced back to you then you can be de-anonymized. If you cannot get this anonymous phone number and/or a physical SIM with a Burner phone, then you will have to restrict yourself to platforms not asking for phone number verification.**

Remember see Appendix N: Warning about smartphones and smart devices

Creating new identities:

This is the fun part where you will now create your identities from thin air. These identities do not exist but should be plausible and look "organic". They should ideally have a story, a "legend" (yes this is the real term for this[349]).

What is a legend? Well, it is a full back-story for your character:

- Age
- Sex
- Gender
- Ethnicity
- Place of Birth and date of Birth
- Place of residence
- Country of origin
- Visited Countries (for travels for instance)
- Interests and hobbies
- Education History
- Work experience
- Health information
- Religion if any
- Goals

---

[347] Wikipedia, Trust but verify https://en.wikipedia.org/wiki/Trust,_but_verify [Wikiless] [Archive.org]

[348] Wikipedia, Zero-trust Security Model https://en.wikipedia.org/wiki/Zero_trust_security_model [Wikiless] [Archive.org]

[349] Wikipedia, Espionage, Organization https://en.wikipedia.org/wiki/Espionage#Organization [Wikiless] [Archive.org]

- Family history
- Family composition if any (Children? Spouse? Husband?)
- Relationship Status if any (Married? Single?)
- Spoken Languages
- Personality traits (Introvert, Extrovert …)
- …

All these should be crafted carefully for every single identity and you should be very careful to stick to the details of each legend when using those identities. Nothing can leak that could lead to your real persona. Nothing could leak that could compromise the consistency of your legend. Everything should always be consistent.

Now is also the moment where you could finally consider getting an online phone number as explained in the Online Phone Number (less recommended) section.

I will help you bit by listing a few tips I learned while doing research over the years **(disclaimer: this is based on my personal experiences alone)**:

- "Some animals are more equal than others".
    - Ethnicity is important and you will have less issues and attract less attention to verification algorithms if your identity is Caucasian/East-Asian than if it is Arabic/Black (yes, I tested this extensively and it is definitely an issue).
    - Age is important and you will have less issues if you are young (18-22) than if you are middle-aged or older. Platforms seem to be more lenient in not imposing restrictions on new younger audiences.
    - Sex/Gender is important and you will have fewer issues if you are a female than if you are a male.
    - Country of origin is important and you will have fewer issues if your identity is Norwegian than if it is Ukrainian, Nigerian, or Mexican.
    - Country of residence is important and you will have fewer issues if your identity has its residence in Oslo or Paris than if you decide to reside in Kiev or Cairo.
    - Language is important and you will have fewer issues if you speak English or the language of your Identity than if you use a non-related language. Do not make a Norwegian born Arabic 20-year-old female that speaks Ukrainian or Arabic.
- Identities that are "EU residents" with an "EU IP" (VPN/Tor Exit IP) will benefit from GDPR protections on many platforms. Others will not. GDPR is your friend in most cases and you should take this into account.
- Similarly, origin IP geolocation (your IP/location when you go to "whatsmyipaddress.com") should match your identity location as much as possible (You can pick this in the VPN client if you use the 3 layers approach or just create a new identity in Tor Browser or Brave Tor Tab until you get the appropriate Exit node, or alternatively configure Tor to restrict your Exit Nodes). You could exclude any exit IP that is not located in Western Europe/US/Canada/Japan/South Korea/Australia/New Zealand as you will have less issues. Ideally, you should get a European Union IP to get additional GDPR protection and if possible, a German exit IP due to their legal stance on using anonymous accounts on online platforms.
- Brave Browser (Chromium based) with a Private Tor Tab has (IMHO) a better acceptance level than Tor Browser (Firefox based). You will experience less issues with captchas and online platforms[340] if you use Brave than if you use Tor Browser (feel free to try this yourself).
- Every identity you should have a matching profile picture associated to it. For this purpose, I recommend you just go to https://thispersondoesnotexist.com/ [Archive.org] and generate a computer-generated profile picture. You can also generate such pictures yourself from your computer if you prefer by using the open-source StyleGan project here https://github.com/NVlabs/stylegan2 [Archive.org]. Just refresh the page until you find a picture that matches your identity in all aspects (age, sex, and ethnicity) and save that picture. It would be even better to have several pictures associated to that identity but I do not have an "easy way" of doing that yet.
    - **Bonus**, you could also make it more real by using this service (with an anonymous identity) https://www.myheritage.com/deep-nostalgia [Archive org] to make a picture more lifelike. Here is an example:
        - Original:

- Result (see Online because PDFs do not work well with embedded media):
  - https://anonymousplanet.github.io/thgtoa/media/after.gif
  - https://mirror.anonymousplanet.github.io/thgtoa/media/after.gif
  - http://thgtoa7imksbg7rit4grgijl2ef6kc7b56bp56pmtta4g354lydlzkqd.onion/media/after.gif
  - Archive.today: https://archive.fo/FB8oV
  - Archive.today over Tor: https://archivecaslytosk.onion/FB8oV

Slight issue tho: **MyHeritrage.com bans Tor Exit nodes so you might have again to consider VPN over Tor for this.**

You could also achieve the same result without using MyHeritage and by doing it yourself using for example https://github.com/AliaksandrSiarohin/first-order-model [Archive.org] but this will require more manual operations (**and requires an NVIDIA GPU**).

Note: If you make several pictures of the same identity using some of the tools mentioned above, be sure to compare the similarities using the Microsoft Azure Face Verification tool at https://azure.microsoft.com/en-us/services/cognitive-services/face/#demo.

- Create in advance and store in KeePassXC each identity details that should include some crafted details:
  - Date of Birth
  - Country of Birth
  - Nationality
  - Country of Residence
  - Address of Residence
  - Languages spoken
  - Occupation (Job Title, University…)
  - Various Interests (Art, Politics, Tech…)
  - Phone number (this is your pre-paid SIM card phone number on your Burner phone or your online number paid with Monero)
- Do not pick an occupation at a well-known private corporations/company as they have people in their HR departments monitoring activities in platforms such as LinkedIn and will report your profile as being fake if it does not match their database. Instead pick an occupation as a freelancer or at a very large public institution where you will face less scrutiny due to their decentralized nature.

- Keep track (write down) of the background stories of your Identities. You should always use the same dates and answers everywhere. Everything should always match up. Even the stories you tell about your imaginary life should always match. If you say you work as an intern at the Department of Health one day and later on another platform, say you work as an intern at the Department of Transportation, people might question your identity. Be consistent.
- Use a different phone number each identity. Online platforms do keep track of phone number usage and if one identity/number gets flagged for violating Community Guidelines or Terms of Services, it might also get the other identities using the same number flagged/banned as well.
- Adapt your language/writing to the identity to not raise suspicions and lower your chances of being fingerprinted by online platforms. Be especially careful with using pedantic words and figures of speech/quotes that could allow some people to guess your writing is very similar to that person with this Twitter handle or this Reddit user.
- Always use TOTP 2FA (not SMS to prevent Sim Swapping attacks[350] and to keep your identity working when your pre-paid card expires) using KeePassXC when available to secure your logins to various platforms.
- Remember Appendix A2: Guidelines for passwords and passphrases.

Here is also a good guide on this specific topic:
https://gendersec.tacticaltech.org/wiki/index.php/Complete_manual#.22Real.22_names [Archive.org]

Note: If you are having trouble finding an Exit node in the country of your choice you can force using specific countries for Exit Nodes (and therefore exit countries) on Tor by editing the torrc file on the Whonix Gateway or even the Tor Browser:

- Whonix/Tails: Create/Edit a file ```/usr/local/etc/torrc.d/50_user.conf```[351].
- On Tor Browser: Edit the torrc file located at ```Browser/TorBrowser/Data/Tor```[352].

Once you are in the file, you can do the following:

- Specify the Exit Nodes by adding those two lines (which will require an Exit Node in China/Russia/Ukraine:
  - ```ExitNodes {CH},{RU},{UA}```
  - ```StrictNodes 1```
- Exclude specific Exit Nodes by adding this line (which will exclude all Exit Nodes from France/Germany/USA/UK):
  - ```ExcludeNodes {FR},{DE},{US},{UK}```

Always use uppercase letter for any setting.

Please note that this is restricting Onion Routing could limit your Anonymity if you are too restrictive. You can see a visualized list of available Exit Nodes here: https://www.bigdatacloud.com/insights/tor-exit-nodes [Archive.org]

Here is the list of possibilities (this is a general list and many of those countries might not have Exit nodes at all):
https://b3rn3d.herokuapp.com/blog/2014/03/05/tor-country-codes/ [Archive.org]

The Real-Name System:

Unfortunately, not using your real identity is against the ToS (Terms of Services) of many services (especially those owned by Microsoft and Facebook). But don't despair, as explained in the Requirements, it's still legal in Germany where the courts have upheld up the legality of not using real names on online platforms (§13 VI of the German Telemedia Act of 2007[1,2]). **Fortunately, ToS cannot override laws (yet)**.

This does not mean that it is illegal in other places but that it might be a breach of their Terms of Services if you do not have the law on your side. **Remember this guide only endorses this for German users residing in Germany.**

---

[350] Wikipedia, Sim Swapping https://en.wikipedia.org/wiki/SIM_swap_scam [Wikiless] [Archive.org]

[351] Whonix Documentation, https://www.whonix.org/wiki/Tor#Edit_Tor_Configuration [Archive.org]

[352] Tor Browser Documentation, https://support.torproject.org/tbb/tbb-editing-torrc/ [Archive.org]

On my side, I strongly condemn this type of real-name policy. See for instance this Wikipedia article giving some examples: https://en.wikipedia.org/wiki/Facebook_real-name_policy_controversy [Wikiless] [Archive.org]

Here are some more references about the German case for reference:

- https://slate.com/technology/2018/02/why-some-americans-are-cheering-germany-for-taking-on-facebooks-real-name-policy.html [Archive.org]
- https://www.theverge.com/2018/2/12/17005746/facebook-real-name-policy-illegal-german-court-rules [Archive org]
- https://www.pcmag.com/news/german-court-rules-facebooks-real-name-policy-is-illegal [Archive org]
- https://www.vzbv.de/sites/default/files/downloads/2018/02/14/18-02-12_vzbv_pm_facebook-urteil_en.pdf [Archive org]
- https://www.pcmag.com/news/german-court-rules-facebooks-real-name-policy-is-illegal [Archive org]
- https://www.reuters.com/article/us-germany-facebook/german-court-rules-facebook-use-of-personal-data-illegal-idUSKBN1FW1FI [Archive.org]

Alternatively, you could be an adult resident of any other country where you can validate and verify the legality of this yourself. Again, this is not legal advice and I am not a lawyer. **Do this at your own risk.**

Other countries where this was ruled illegal

- South Korea (see https://en.wikipedia.org/wiki/Real-name_system#South_Korea [Wikiless] [Archive.org])
- If you know any other, please let me know with references in the GitHub issues.

Some platforms are by-passing this requirement all-together by requiring a valid payment method instead (see Financial transactions:). While this does not directly require a real-name through their ToS, this has the same results as they usually only accept mainstream (not Monero/Cash) payment methods (such as Visa/MasterCard/Maestro or PayPal) which do require a real-name legally as part of their KYC[213] regulations. The result is the same and arguably even better than a simple real-name policy you could ignore in some countries such as Germany.

About paid services:

If you intend to use paid services, privilege those accepting cash payments or Monero payments which you can do directly and safely while keeping your anonymity.

If the service you intend to buy does not accept those but accepts Bitcoin (BTC), consider the following appendix: Appendix Z: Paying anonymously online with BTC.

Overview:

This section will show you an overview of the current various requirements on some platforms.

- **Consider using the recommended tools on https://privacytools.io/ [Archive.org] for your better privacy instead of the usual mainstream ones.**
- **Consider using the recommended tools on https://www.whonix.org/wiki/Documentation [Archive org] as well instead of the usual mainstream ones such as E-mail providers: https://www.whonix.org/wiki/E-Mail#Anonymity_Friendly_Email_Provider_List [Archive org]**

The following overview does not mention the privacy practices of those platforms but only their requirements for registering an account. If you want to use privacy-aware tools and platforms, head on to https://privacytools.io/ [Archive org]

Legend:

- "Unclear": Unclear due to lack of information or confusing information.
- "Maybe": It did happen in a minority of my tests.
- "Likely": It did happen in most of my tests.
- "Yes" or "No": This either happened or never happened systematically in all my tests.
- "Easy": The overall experience was straightforward with little to no obstacles.
- "Medium": The overall experience has some obstacles but it is still doable without too much hassle.

- "Hard": The overall experience is a painful struggle with many obstacles.
- "N/A": Not Applicable because it was not possible to test within the context of this guide
- "Indirectly": This means they do require something but indirectly through a third-party system (Financial KYC for example).

Service	Against ToS	Requires Phone	Requires E-Mail	VPN Sign-up	Tor Sign-up	Captchas	ID or Financial Checks	Facial Checks	Manual Checks	Overall difficulty
Amazon	No	No	Yes	Yes	Yes	No	Yes*	No	Unclear	N/A
Apple	Yes*	Yes	Yes	Yes	Yes	No	No	No	No	Medium
Briar	No	No	No	Yes	Yes	No	No	No	No	Easy
Discord	No	No	Yes	Yes	Yes	Yes	No	No	No	Medium
Element	No	No	No	Yes	Yes	Yes	No	No	No	Easy
Facebook	Yes*	Yes	Yes	Maybe	Maybe	Yes	Maybe	Maybe	Maybe	Hard
GitHub	No	No	Yes	Yes	Yes	Yes	No	No	No	Easy
GitLab	No	No	Yes	Yes	Yes	Yes	No	No	No	Easy
Google	No	Likely	Likely	Yes	Yes	Yes	Maybe	No	Maybe	Medium
HackerNews	No	No	No	Yes	Yes	Yes	No	No	No	Easy
Instagram	Unclear	Likely	Yes	Yes	Yes	Yes	No	Maybe	Maybe	Medium
Jami	No	No	No	Yes	Yes	No	No	No	No	Easy
iVPN	No	No	No	Yes	Yes	No	No	No	No	Easy
LinkedIn	Yes*	Yes	Yes	Yes	Yes	Yes	Maybe	Maybe	Maybe	Hard
MailFence	No	No	Yes	Yes	Maybe	Yes	No	No	No	Medium
Medium	No	No	Yes	Yes	Yes	No	No	No	No	Easy
Microsoft	Yes*	Maybe	Maybe	Yes	Yes	Yes	No	No	No	Medium
Mullvad	No	No	No	Yes	Yes	No	No	No	No	Easy
Njalla	No	No	No	Yes	Yes	No	No	No	No	Easy
OnionShare	No	No	No	Yes	Yes	No	No	No	No	Easy
ProtonMail	No	Maybe	Likely	Yes	Yes	Yes	No	No	No	Medium
ProtonVPN	No	No	Yes	Yes	Yes	No	No	No	No	Medium
Reddit	No	No	No	Yes	Yes	No	No	No	No	Easy
Slashdot	Yes*	No	No	Yes	Yes	Yes	No	No	No	Medium
Telegram	No	Yes	No	Yes	Yes	No	No	No	No	Easy
Tutanota	No	No	No	Maybe	No	Yes	No	No	No	Hard
Twitch	No	No	Yes	Yes	Yes	Yes	No	No	No	Easy
Twitter	No	Likely	Yes	Yes	Yes	Yes	No	No	Maybe	Medium
WhatsApp	Yes*	Yes	No	Yes	Yes	No	No	No	No	Medium
4chan	No	No	No	No	No	Yes	No	No	No	Hard

*** See The Real-Name System for important information.**

Amazon:

- Is this against their ToS? No but yes
  https://www.amazon.com/gp/help/customer/display.html?nodeId=202140280 [Archive.org]

"1. Amazon Services, Amazon Software

A. Use of Amazon Services on a Product. To use certain Amazon Services on a Product, you must have your own Amazon.com account, be logged in to your account on the Product, **and have a valid payment method associated with your account.** "

While it does not technically require a real-name. It does require a valid payment method. Unfortunately, it will not accept "cash" or "Monero" as a payment method. So instead, they are relying on financial KYC (where a real-name policy is pretty much enforced everywhere).

- Will they require a phone number? No

- Can you create accounts through Tor? Yes

Because of this valid payment method requirement, I could not test this. While this is seemingly not against their ToS, it is not possible within the context of this guide unless you manage to obtain a valid KYC payment method anonymously which AFAIK is pretty much impossible or extremely difficult.

Apple:

- Is this against their ToS? Yes https://www.apple.com/legal/internet-services/icloud/en/terms.html [Archive.org]

"IV. Your Use of the Service

A. Your Account

In order to use the Service, you must enter your Apple ID and password to authenticate your Account. **You agree to provide accurate and complete information when you register with, and as you use, the Service ("Service Registration Data"), and you agree to update your Service Registration Data to keep it accurate and complete".**

- Will they require a phone number? Yes
- Can you create accounts through Tor? Yes

Briar:

- Is this against their ToS? https://briarproject.org/privacy-policy/ [Archive.org]
- Will they require a phone number? No, they do not even require an e-mail
- Can you create accounts through Tor? Yes

Note that this app requires an Android emulator for all features. There is no stable desktop client yet. However, you can install a beta version (with some limited features) on Linux following this guide: https://code.briarproject.org/briar/briar-gtk

Discord:

- Is this against their ToS? https://discord.com/terms [Archive.org]
- Will they require a phone number? No but they do require an e-mail
- Can you create accounts through Tor? I had no issues with that so far using the Desktop Client

You might encounter more issues using the Web Client (Captchas). Especially with Tor Browser.

I suggest using the Discord Client app on a VM through Tor or ideally through VPN over Tor to mitigate such issues.

Steps after creating: Enable 2FA authentication with KeePassXC TOTP

Element:

- Is this against their ToS? https://element.io/terms-of-service [Archive.org]
- Will they require a phone number? No, they do not even require an e-mail
- Can you create accounts through Tor? Yes

Expect some Captchas during account creation.

Facebook:

- Is this against their ToS? Yes https://www.facebook.com/terms.php [Archive org]

"1. Who can use Facebook

When people stand behind their opinions and actions, our community is safer and more accountable. For this reason, you must:

- Use the same name that you use in everyday life.
- Provide accurate information about yourself.
- Will they require a phone number? Yes, and probably more later

- Can you create accounts through Tor? Yes, but it is very difficult and their onion address[353] will not help. In most cases you'll just have a random error at sign-up and your account suspended after sign-in."

But this clause of their ToS is illegal in Germany (see Requirements).

Facebook is one of the most aggressive platforms in identity verification and is pushing hard their "real name policy". It is why this guide is only advised to German residents.

Over my tests tho I was able to pinpoint a few tips:

- It will be easier if you have an Instagram account first.
- Signing-up through Tor is almost impossible and will only succeed if you are "lucky" (I assume if you are using an exit Node that is not yet known by Facebook verification systems). It will not allow registration at all and will just fail with "An error has occurred during registration".
- Signing-up through VPNs is more likely to succeed but might still result in the same error. So, you must be ready for a lot of trial and errors here.
- My previous entry in the guide about the Orwellian quote from Animal Farm is in full effect on Facebook. You will experience huge variation in acceptance depending on age/sex/ethnicity/nationality/… This is where you will have far less issues if you are making an account of a Young European Caucasian Female. You will almost certainly fail if you try making a Middle-Aged Male where my other accounts are still unsuspended/unbanned to this day.
- Logging-in (after you sign-up) however works fine with VPN and Tor but might still get your account suspended for violating Community Guidelines or Terms of Services (despite you not using the account at all for anything else than signing-up/logging-in).

I also suspect strongly based on my test that the following points have an impact on your likelihood of being suspended over time:

- Not having friends
- Not having interests and an "organic activity"
- Not being in the contacts of any other user
- Not being on other platforms (such as Instagram/WhatsApp)
- Restricting your profile privacy settings too soon after signing-up

If your account gets suspended, you will need to appeal the decision through a very simple form that will require you to submit a "proof of ID". However, that proof of ID verification system is more lenient than LinkedIn and will allow you send various documents which require far less Photoshop skills.

It is also possible that they ask you to take a selfie video or picture making certain gestures to prove your identity. If that is the case, I am afraid it is a dead end for now.

If you do file an appeal, you will have to wait for Facebook to review it (I do not know if this is automatic or human) and you will have to wait and hope for them to unsuspend your account.

GitHub:

- Is this against their ToS? https://docs.github.com/en/free-pro-team@latest/github/site-policy/github-terms-of-service [Archive.org]
- Will they require a phone number? Nope, all good
- Can you create accounts through Tor? Yes, but expect some captchas

GitHub is straightforward and requires no phone number.

Just Sign-up with e-mail and password and enable two-factor authentication (TOTP in KeePassXC). By default, your e-mail will be private.

[353] Facebook Onion Website http://facebookcorewwwi.onion

Be sure to go into Settings > E-Mail and make your e-mail private as well as block any push that would reveal your e-mail.

GitLab:

- Is this against their ToS? https://about.gitlab.com/handbook/legal/subscription-agreement/ [Archive org]
- Will they require a phone number? Nope, all good
- Can you create accounts through Tor? Yes, but expect captchas

GitLab is straightforward and requires no phone number.

Just Sign-up with e-mail and password and enable two-factor authentication (TOTP in KeePassXC). By default, your e-mail will be private.

Google:

- Is this against their ToS? https://policies.google.com/terms [Archive.org]
- Will they require a phone number? Yes, they will. There is no escape here.
- Can you create accounts through Tor? Yes, but expect some captchas and your phone number will be required

ProtonMail is good … but to appear less suspicious, it is just better to also have a mainstream Google Mail account.

As ProtonMail, Google will also most likely require a phone number during sign-up as part of their verification process. However contrary to ProtonMail, Google will store that phone number during the sign-up process and will also limit the number of accounts that can be created during the sign-up[354,355].

From my experience during my research, this count is limited to 3 accounts / phone number. If you are unlucky with your number (if it was previously used by another mobile user), it might be less.

You should therefore use again your online phone number OR your burner phone and pre-paid SIM card to create the account. Do not forget to use the identity details you made up earlier (birthdate). When the account is created, please do take some time to do the following:

- Log into Google Mail and Go into the Gmail Settings > Go into the mail Forwarding options > Set up a mail forwarding to your ProtonMail Address > Verify (using ProtonMail) > Go back to Gmail and set the forwarding to forward and delete Google copy > Save. This step will allow you to check your Google Mail using ProtonMail instead and will allow you to avoid triggering Google Security checks by Logging in from various VPN/Tor exit IP addresses in the future while storing your sensitive e-mail at ProtonMail instead.
- Enable 2FA within the Google account settings. First, you will have to enable 2FA using the phone number. Then you will see the option appear to enable 2FA using an Authenticator app. Use that option and set it up with a new KeePassXC TOTP entry. When it is done, remove the phone 2FA from the Google account. This will prevent someone from using that phone number in the future (when you do not have it anymore) to recover/gain access to that account.
- Add ProtonMail as a recovery e-mail address for the account.
- Remove the phone number from the account details as a recovery option.
- Upload a Google profile picture you made earlier during the identity creation step.
- Review the Google Privacy settings to disable as much as you can:
    - Activity logging
    - YouTube
- Log out and do not touch it unless needed (as mentioned, you will use ProtonMail to check your Gmail).

Keep in mind that there are different algorithms in place to check for weird activity. If you receive any mail (on ProtonMail) prompting about a Google Security Warning. Click it and click the button to say "Yes it was me". It helps.

---

[354] Google Help https://support.google.com/accounts/answer/114129?hl=en [Archive.org]

[355] Google Help https://support.google.com/google-ads/answer/7474263?hl=en [Archive.org]

Do not use that account for "sign-up with Google" anywhere unless necessary.

Be extremely careful if you decide to use the account for Google activities (such as Google Maps reviews or YouTube Comments) as those can easily trigger some checks (Negative reviews, Comments breaking Community Guidelines on YouTube).

If your account gets suspended [356] (this can happen on sign-up, after signing-up or after using it in some Google services), you can still get it unsuspended by submitting[357] an appeal/verification (which will again require your Phone number and possibly an e-mail contact with Google support with the reason). Suspension of the account does not disable the e-mail forwarding but suspended account will be deleted after a while.

After suspension, if your Google account is restored, you should be fine.

If your account gets banned, you will have no appeal and the forwarding will be disabled. Your phone number will be flagged and you will not be able to use it to sign-up on a different account. Be careful when using those to avoid losing them. They are precious.

It is also possible that Google will require an ID check through indirect financial KYC or ID picture check if you attempt to access/publish mature content on their platform[358].

HackerNews:

- Is this against their ToS? https://www.ycombinator.com/legal/#tou [Archive.org]
- Will they require a phone number? No, they do not even require an e-mail
- Can you create accounts through Tor? Yes

Instagram:

- Is this against their ToS? **Maybe?** I am not sure https://help.instagram.com/581066165581870?ref=dp [Archive org]

"You can't impersonate others or provide inaccurate information. You do not have to disclose your identity on Instagram, but you must provide us with accurate and up to date information (including registration information). Also, you may not impersonate someone you are not, and you can't create an account for someone else unless you have their express permission".

This one is a bit of an Oxymoron do not you think? So, I am not sure if it is allowed or not.

- Will they require a phone number? Maybe but less likely over VPN and very likely over Tor
- Can you create accounts through Tor? Yes, but expect some captchas and your phone number will be required

It is also possible that they ask you to take a selfie video or picture making certain gestures to prove your identity (within the app or through an e-mail request). If that is the case, I am afraid it is a dead end for now.

It is no secret that Instagram is part of Facebook however it is more lenient than Facebook when it comes to user verification. It is quite unlikely you will get suspended or banned after signing-up. But it could help.

For instance, I noticed that you will have less issues creating a Facebook account if you already have a valid Instagram account. You should always create an Instagram account before attempting Facebook.

Unfortunately, there are some limitations when using the web version of Instagram. For instance, you will not be able to enable Authenticator 2FA from the web for a reason I do not understand.

---

[356] Google, Your account is disabled https://support.google.com/accounts/answer/40695 [Archive.org]

[357] Google, Request to restore the account https://support.google.com/accounts/contact/disabled2 [Archive.org]

[358] Google Help, Update your account to meet age requirements https://support.google.com/accounts/answer/1333913?hl=en [Archive org]

After sign-up, do the following:

- Upload a picture of your generated identity if you want.
- Go into your Settings
- Make the account private (initially at least)
- Do not show activity status
- Do not allow sharing

Jami:

- Is this against their ToS? https://jami.net/privacy-policy/ [Archive org]
- Will they require a phone number? No, they do not even require an e-mail
- Can you create accounts through Tor? Yes

iVPN:

- Is this against their ToS? https://www.ivpn.net/tos/ [Archive.org]
- Will they require a phone number? No, they do not even require an e-mail
- Can you create accounts through Tor? Yes

LinkedIn:

- Is this against their ToS? Yes https://www.linkedin.com/legal/user-agreement [Archive org]

"To use the Services, you agree that: (1) you must be the "*Minimum Age*" (described below) or older; (2) **you will only have one LinkedIn account, which must be in your real name**; and (3) you are not already restricted by LinkedIn from using the Services. **Creating an account with false information is a violation of our terms**, including accounts registered on behalf of others or persons under the age of 16. "

But this clause of their ToS is illegal in Germany (see Requirements).

- Will they require a phone number? Yes, they will.
- Can you create accounts through Tor? Yes, but expect some captchas and your phone number will be required

LinkedIn is far less aggressive than twitter but will nonetheless require a valid e-mail (preferably again your Gmail) and a phone number in most cases (tho not always).

LinkedIn however is relying a lot on reports and user/customer moderation. You should not create a profile with an occupation inside a private corporation or a small startup company. The company employees are monitoring LinkedIn activity and receive notifications when new people join. They can then report your profile as fake and your profile will then be suspended or banned pending appeal.

LinkedIn will then require you go through a verification process that will unfortunately require you to send an ID proof (identity card, passport, driver license). This ID verification is processed by a company called Jumio[359] that specializes in ID proofing. This is most likely a dead end as this would force you to develop some strong Photoshop skills.

Instead, you are far less likely to be reported if you just stay vague (say you are a student/intern/freelance) or pretend you work for a large public institution that is too large for anyone to care of check.

As with Twitter and google, you should do the following after signing-up:

- Disable ads
- Disable notifications
- Disable lookup by phone/e-mail
- Upload a picture of your identity

[359] Jumio, ID verification features https://www.jumio.com/features/ [Archive.org]

MailFence:

- Is this against their ToS? No
- Will they require a phone number? No but they require an e-mail
- Can you create accounts through Tor? Maybe. From my tests, the signing-up verification e-mails are not sent when using Tor to sign-up.

Medium:

- Is this against their ToS? No unless it is about crypto https://policy.medium.com/medium-terms-of-service-9db0094a1e0f [Archive.org]
- Will they require a phone number? No but they require an e-mail
- Can you create accounts through Tor? I had no issues with that so far

Signing-in does require an e-mail every time.

Microsoft:

- Is this against their ToS? Yes https://www.microsoft.com/en/servicesagreement/ [Archive.org]

"i. Creating an Account. You can create a Microsoft account by signing up online. **You agree not to use any false, inaccurate or misleading information when signing up for your Microsoft account".**

But this clause of their ToS is illegal in Germany (see Requirements).

- Will they require a phone number? Likely but not always. Depending on your luck with you Tor exit node, it is possible that they will only require e-mail verification. If you use a VPN over Tor, they will likely only ask an e-mail.
- Can you create accounts through Tor? Yes, you can but expect captchas, at least e-mail verification, **and likely phone verification.**

So yes, it is still possible to create an MS account without a phone number and using Tor or VPN but you might have cycle through a few exit nodes to achieve this.

After signing-up you should setup 2FA authentication within security and using KeePassXC TOTP.

Mullvad:

- Is this against their ToS? No https://mullvad.net/en/help/terms-service/ [Archive.org]
- Will they require a phone number? No, they do not even require an e-mail.
- Can you create accounts through Tor? Yes.

Njalla:

- Is this against their ToS? No https://njal.la/tos/ [Archive org]
- Will they require a phone number? No but they do require an e-mail or an XMPP (Jabber) account somewhere.
- Can you create accounts through Tor? Yes, they even have an ".onion" address at http://njalladnspotetti.onion

OnionShare:

- Is this against their ToS? No, they do not even have Terms of Services
- Will they require a phone number? No, they do not even require an e-mail
- Can you create accounts through Tor? Yes (obviously)

ProtonMail:

- Is this against their ToS? No https://ProtonMail.com/terms-and-conditions [Archive.org]
- Will they require a phone number? Maybe. This depends on the IP you are coming from. If you come from Tor, it is likely. From a VPN, it is less likely.
- Can you create accounts through Tor? Yes, but very likely that a phone number will be required when only an e-mail will be over a VPN. They even have an ".onion" address at https://protonirockerxow.onion/.

You obviously need an e-mail for your online identity and disposable e-mails are pretty much banned everywhere.

ProtonMail is a free e-mail provider based in Switzerland that advocates security and privacy.

They are recommended by privacytools.io[360]. Their only apparent issue is that they do require (in most cases) a phone number or another e-mail address for registration (when you try to register from a VPN or Tor at least).

They claim they do not store/link the phone/e-mail associated with the registration but only store a hash that is not linked to the account[361]. If their claim is true and the hash is not linked to your account, and that you followed my guide regarding the phone number, you should be reasonably safe from tracking.

Create this e-mail account first using the phone as verification if necessary.

When you are done creating the account, please go into the settings and enable 2FA (Two Factor Authentication). You will use KeePassXC TOTP feature (create a new entry "Identity ProtonMail TOTP" and just use the TOTP menu to set it up). Save the rescue codes within your KeePassXC entry.

This e-mail account will be used in the next step for creating a Google/Gmail account.

ProtonVPN:

- Is this against their ToS? No https://protonvpn.com/terms-and-conditions [Archive.org]
- Will they require a phone number? No but they do require an e-mail.
- Can you create accounts through Tor? Yes

Reddit:

- Is this against their ToS? No https://www.redditinc.com/policies [Archive.org]
- Will they require a phone number? No, they will not.
- Can you create accounts through Tor? Yes

Reddit is simple. All you need to register is a valid username and a password. Normally they do not even require an e-mail (you can skip the e-mail when registering leaving it blank).

You should still enable 2FA in the settings after signing-up. I had no issues whatsoever signing-up over Tor or VPN besides the occasional Captchas.

Slashdot:

- Is this against their ToS? Yes https://slashdotmedia.com/terms-of-use/ [Archive.org]

"

8. Registration; Use of Secure Areas and Passwords

Some areas of the Sites may require you to register with us. When and if you register, you agree to (a) provide accurate, current, and complete information about yourself as prompted by our registration form (including your e-mail address) and (b) to maintain and update your information (including your e-mail address) to keep it accurate, current, and complete. You acknowledge that should any information provided by you be found to be untrue, inaccurate, not current, or incomplete, we reserve the right to terminate this Agreement with you and your current or future use of the Sites (or any portion thereof)".

- Will they require a phone number? No
- Can you create accounts through Tor? Yes

Telegram:

- Is this against their ToS? No https://telegram.org/tos [Archive.org]
- Will they require a phone number? Yes unfortunately
- Can you create accounts through Tor? Yes, but sometimes you randomly get banned without any reason

Telegram is quite straightforward and you can download their portable Windows app to sign-up and login.

---

[360] Privacytools.io Recommended E-mail Providers https://privacytools.io/providers/email/ [Archive.org]

[361] ProtonMail Human Verification System https://ProtonMail.com/support/knowledge-base/human-verification/ [Archive org]

It will require a phone number (that can only be used once) and nothing else.

In most cases I had no issues whether it was over Tor or VPN but I had a few cases where my telegram account was just banned for violating terms of services (not sure which one?). This again despite not using them for anything.

They provide an appeal process through e-mail but I had no success with getting any answer.

Their appeal process is just sending an e-mail to recover@telegram.org [Archive.org] stating your phone number and issue and hope they answer.

After signing-up you should do the following:

- Go into Edit profile
- Set a Username
- Go into Settings (Desktop App)
- Set the Phone Number visibility to Nobody
- Set Last Seen & Online to Nobody
- Set Forwarded Messages to Nobody
- Set Profile photos to Contacts
- Set Calls to Contacts
- Set Group & Channels to Contacts

Tutanota:

- Is this against their ToS? No https://tutanota.com/terms/ [Archive.org]
- Will they require a phone number? No but they do require an e-mail.
- Can you create accounts through Tor? Not really, almost all Tor Exit nodes are banned AFAIK

Twitter:

- Is this against their ToS? No https://twitter.com/en/tos
- Will they require a phone number? They might not at sign-up but they will just after sign-up or later.
- Can you create accounts through Tor? Yes, but expect some captchas and your phone number will be required after a while.

Twitter is extremely aggressive in preventing anonymity on their network. You should sign-up using e-mail and password (not phone) and not using "Sign-in with Google". Use your Gmail as the e-mail address.

More than likely, your account will be suspended immediately during the sign-up process and will require you to complete a series of automated tests to unlock. This will include a series of captchas, confirmation of your e-mail and twitter handle or other information. In some cases, it will also require your phone number.

In some cases, despite you selecting a text verification, Twitter verification system will call the phone no matter what. In that case you will have to pick up and hear the verification code. I suspect this is another method of preventing automated systems and malicious users from selling text receiving services over the internet.

Twitter will store all this information and link it to your account including your IP, e-mail, and phone number. You will not be able that phone number to create a different account.

Once the account is restored, you should take some time to do the following:

- Upload the identity profile picture.
- Enable 2FA from the security settings using a new KeePassXC TOTP entry, save the security codes in KeePassXC as well.
- Disable Photo tagging
- Disable E-mail lookup
- Disable Phone lookup
- Disable all personalized advertising settings
- Disable geolocation of tweets
- Remove the phone number from the account

- Follow some people based
- Log out and leave it be.

After about a week, you should check the twitter again and the chances are quite high that it will be suspended again for "suspicious activity" or "violating community guidelines" despite you not using it at all (not even a single tweet/follow/like/retweet or DM) but this time by another system. I call this the "Double tap".

This time you will need to submit an appeal using a form[362], provide a good reason and wait for the appeal to be processed by Twitter. During that process, it is possible that you will receive an e-mail (on ProtonMail) asking you to reply to a customer service ticket to prove that you do have access to your e-mail and that it is you. This will be directed toward your Gmail address but will arrive on your ProtonMail.

Obviously do not reply from ProtonMail as this will raise suspicions, you must sign-in into Gmail (unfortunately) and compose a new mail from there copy pasting the E-Mail, Subject and Content from ProtonMail. As well as a reply confirming you have access to that e-mail.

After a few days, your account should get unsuspended "for good". I had no issues after that but keep in mind they can still ban your account for any reason if you violate the community guidelines. The phone number and e-mail will then be flagged and you will have no other option but to get a new identity with a new number to sign-up again. Do not use this account for trolling.

Twitch:

- Is this against their ToS? No https://www.twitch.tv/p/en/legal/terms-of-service/ [Archive.org]
- Will they require a phone number? No but they do require an e-mail.
- Can you create accounts through Tor? Yes

Note that you will not be able to enable 2FA on Twitch using only e-mail. This feature requires a phone number to enable.

WhatsApp:

- Is this against their ToS? **Yes** https://www.whatsapp.com/legal/updates/terms-of-service-eea [Archive.org]

"**Registration**. You must register for our Services **using accurate information**, provide your current mobile phone number, and, if you change it, update your mobile phone number using our in-app change number feature. You agree to receive text messages and phone calls (from us or our third-party providers) with codes to register for our Services".

- Will they require a phone number? Yes, obviously they do.
- Can you create accounts through Tor? I had no issues with that so far.

4chan:

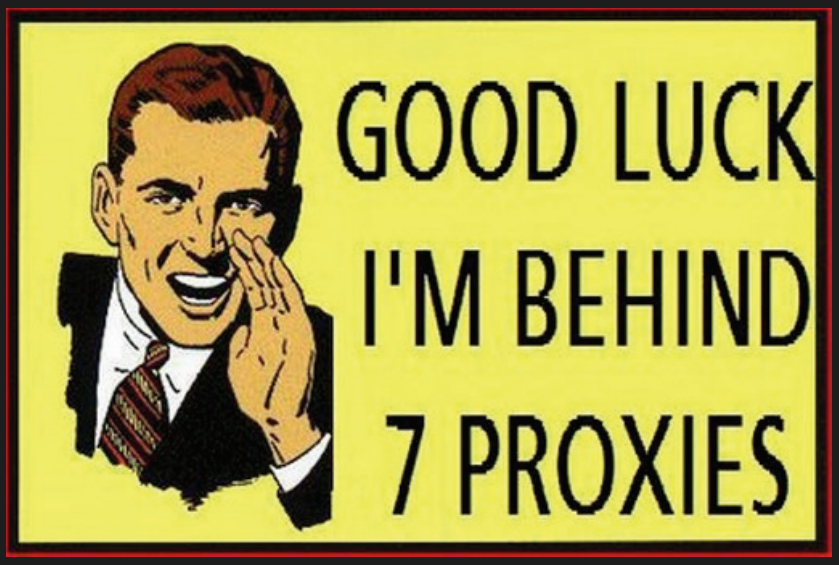
- Is this against their ToS? No
- Will they require a phone number? No, they will not.
- Can you post there with Tor or VPN? Not likely.

4chan is 4chan … This guide will not explain 4chan to you. They block Tor exit nodes and known VPN IP ranges.

You are going to have to find a different way to post there using at least seven proxies[363] that are not known by 4chan blocking system (hint: Anonymous VPS using Monero is probably your best option).

[362] Twitter Appeal Form https://help.twitter.com/forms/general

[363] KnowYourMeme, Good Luck, I'm Behind 7 Proxies https://knowyourmeme.com/memes/good-luck-im-behind-7-proxies [Archive org]



Crypto Wallets:

Use any crypto wallet app within the Windows Virtual Machine. But be careful not to transfer anything toward an Exchange or a known Wallet. Crypto is in most case NOT anonymous and can be traced back to you when you buy/sell any (remember the Your Crypto currencies transactions section).

If you really want to use Crypto, use Monero which is the only one with reasonable privacy/anonymity.

Ideally, you should find a way to buy/sell crypto with cash from an unknown person.

What about those mobile only apps (WhatsApp/Signal)?

There are only three ways of securely using those anonymously (that I would recommend). Using a VPN on your phone is not among those ways. All of those are unfortunately "tedious" to say the least.

- Use an Android Emulator within the Windows VM and run the App through your multi-layer of Tor/VPN. Drawback is that such emulators are usually quite resource hungry and will slow down your VM and use more battery. Here is also an (outdated) guide on this matter: https://www.bellingcat.com/resources/how-tos/2018/08/23/creating-android-open-source-research-device-pc/ [Archive.org]. As for myself I will recommend the use of x86 Android on Virtualbox (see https://www.android-x86.org/documentation/virtualbox.html [Archive org]) that you can also set-up easily.
- Use a non-official app (such as Wassapp for WhatsApp) to connect from the Windows VM to the app. But at your own risk as you could get banned for violating the terms of services by using a non-official App.
- (Not recommended and most complicated) Have a burner Smartphone that you will connect to the VM layered network through Tethering/Sharing of the connection through Wi-Fi. I will not detail this here but it is an option if you really want to.

There is no way to reliably set this multi-layered connectivity approach easily on an Android phone (it is not even possible on IOS as far as I know). By reliable I mean being sure that the smartphone will not leak anything such as geolocation or anything else from booting up to shutting down.

Anything else:

You should use the same logic and security for any other platform that with these mentioned in this guide.

It should work in most cases with most platforms. **The hardest platform to use with full anonymity is Facebook.**

This will obviously not work with banks and most financial platforms (such as PayPal or Crypto Exchanges) requiring actual real official and existing identification. This guide will not help you there as this would be illegal in most places.

How to share files or chat anonymously:

There are plenty of messaging apps everywhere. Some have excellent UI and UX and terrible Security/Privacy. Some have excellent Security/Privacy but terrible UI and UX. It is not easy to pick the ones that you should use for sensitive activities. So, this section will help you do that.

Before going further, there are also some key basic concepts you need to understand:

End-to-end Encryption:
End-to-end Encryption[364] (aka e2ee) is a rather simple concept. It just means only you and your destination know each-others public encryption keys and no one in between that would be eavesdropping would be able to decrypt the communication.

However, the term is often used differently depending on the provider:

- Some providers will claim e2ee but forget to mention what is covered by their protocols. For instance, is metadata also protected within their e2ee protocol? Or is just the content of the messages?
- Some providers do provide e2ee but only as an opt-in option (disabled by default).
- Some providers do offer e2ee with 1 to 1 messaging but not with group messaging.
- Some providers will claim the use of e2ee but their proprietary apps are closed-source where no one can actually verify the claim and the strength of the encryption used.

For these reasons, it is always important to check the claims of various apps. Open-Source apps should always be preferred to verify what kind of encryption they are using and if their claims are true. If not open-source, such apps should have an openly available independent (made by a reputable third party) report validating their claims.

Roll your own crypto:
See the Bad Cryptography section at the start of this guide.

Always be cautious of apps rolling their own crypto until it has been reviewed by many in the crypto community (or even better published and peer reviewed academically). Again, this is harder to verify with closed-source proprietary apps.

It is not that rolling your own crypto is bad in essence, it is that good cryptography needs real peer reviewing, auditing, testing… And since you are probably not a cryptanalyst (and obviously I am not one either), chances are high we are not competent to assess the cryptography of some app.

Forward Secrecy:
Forward Secrecy[365] (FS aka PFS for Perfect Forward Secrecy) is a property of the key agreement protocol of some of those messaging apps and is a companion feature of e2ee. This happens before you establish communication with the destination. The "Forward" refers to the future in time and means that every time you establish a new e2ee communication, a new set of keys will be generated for that specific session. The goal of forward secrecy is to maintain secrecy of past communications (sessions) even if the current one is compromised. If an adversary manages to get hold of your current e2ee keys, that adversary will then be limited to the content of the single session and will not be able to easily decrypt past ones.

This has some user experience drawbacks like for instance a new device could not be able to conveniently access the remotely stored chat history without additional steps.

So, in short, Forward Secrecy protects past sessions against future compromises of keys or passwords.

More on this topic on this YouTube video: https://www.youtube.com/watch?v=zSQtyW_ywZc [Invidious]

Some providers and apps claiming to offer e2ee do not offer FS/PFS sometimes for usability reasons (group messaging for instance is more complex with PFS). It is therefore important to prefer open-source apps providing forward secrecy to those that do not.

---

[364] Wikipedia, end-to-end encryption, https://en.wikipedia.org/wiki/End-to-end_encryption [Wikiless] [Archive.org]

[365] Wikipedia, Forward Secrecy, https://en.wikipedia.org/wiki/Forward_secrecy [Wikiless] [Archive.org]

Zero-Access Encryption at rest:

Zero-Access Encryption[366] at rest is used when you store data at some provider (let us say your chat history or chat backups) but this history or backup is encrypted on your side and cannot be read or decrypted by the provider hosting it.

Zero-Access encryption is an added feature/companion to e2ee but is applied mainly to data at rest and not communications.

Examples of this issue would be iMessage and WhatsApp, see the Your Cloud backups/sync services at the start of this guide.

So again, it is best to prefer Apps/Providers that do offer Zero-Access Encryption at rest and cannot read/access any of your data/metadata even at rest and not only limited to communications.

Such feature would have prevented important hacks such as the Cambridge Analytica scandal[367] if it was implemented.

Metadata Protection:

Remember the Your Metadata including your Geo-Location section. End-to-end Encryption is one thing but it does not necessarily protect your metadata.

For Instance, WhatsApp might not know what you are saying but they might know who you are talking to, how long and when you have been talking to someone, who else is in groups with you, and if you transferred data with them (such as large files).

End-to-end Encryption does not in itself protect an eavesdropper from harvesting your metadata.

This data can also be protected/obfuscated by some protocols to make metadata harvesting substantially harder for eavesdroppers. This is the case for instance with the Signal Protocol which does offer some added protection with features like:

- The Sealed Sender option[368].
- The Private Contact Discovery[369].
- The Private Group System[370].

Other Apps like Briar or OnionShare will protect metadata by using the Tor Network as a shield and storing everything locally on-device. Nothing is stored remotely and all communications are either direct using proximity wi-fi/Bluetooth or remotely through the Tor network.

Most apps however and especially closed-source proprietary commercial apps will collect and retain your metadata for various purposes. And such metadata alone is enough to figure out a lot of things about your communications.

Again, it is important to prefer open-source apps with privacy in mind and various methods in place to protect not only the content of communications but all the associated metadata.

Open-Source:

Finally, Open-Source apps should always be preferred because they allow third parties to check actual capabilities and weaknesses vs claims of marketing departments. Open-Source does not mean the app should be free or non-commercial. It just means transparency.

---

[366] Protonblog, What is zero-access encryption and why it is important for security https://protonmail.com/blog/zero-access-encryption/ [Archive org]

[367] Wikipedia, Cambridge Analytica Scandal, https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal [Wikiless] [Archive.org]

[368] Signal Blog, Technology preview: Sealed sender for Signal https://signal.org/blog/sealed-sender/ [Archive.org]

[369] Signal Blog, Private Contact Discovery, https://signal.org/blog/private-contact-discovery/ [Archive.org]

[370] Signal Blog, Private Group System, https://signal.org/blog/signal-private-group-system/ [Archive.org]

Comparison:

Below you will find a small table showing the state of messaging apps as of the writing of this guide based on my tests and data from the various sources below:

- Wikipedia, https://en.wikipedia.org/wiki/Comparison_of_instant_messaging_protocols [Wikiless] [Archive.org]
- Wikipedia, https://en.wikipedia.org/wiki/Comparison_of_cross-platform_instant_messaging_clients [Wikiless] [Archive org]
- Secure Messaging Apps https://www.securemessagingapps.com/ [Archive.org]
- ProtonMail Blog, https://protonmail.com/blog/whatsapp-alternatives/ [Archive.org]
- Whonix Documentation, Instant Messenger Chat https://www.whonix.org/wiki/Chat [Archive.org]

App[0]	e2ee[1]	Roll Your Own Crypto	Perfect Forward Secrecy	Zero-Access Encryption at-rest[5]	Metadata Protection (obfuscation, encryption …)	Open-Source	Default Privacy Settings	Native Anonymous Sign-up (no e-mail or phone)	Possible through Tor	Privacy and Security Track Record ***	De-centralized
Briar (preferred)	Yes	No [371]	Yes	Yes	Yes (strong)	Yes	Medium (disable wi-fi and Bluetooth)	Yes	Natively[2] (Disable wi-fi and BT) or Virtualization	Good	Yes (peer to peer)
Discord (avoid)	No	Closed-source[6]	No	No	No	No	Bad	E-Mail Required	Virtualization	Bad	No
Element / Matrix.org (preferred)	Yes (opt-in)	No	Yes	Yes	Poor[372]	Yes	Good	Yes	Via Proxy[2] or Virtualization	Good	Partial (federated servers)
Facebook Messenger (avoid)	Partial (Only 1to1 / opt-in)	Closed-source[6]	Yes	No	No	No	Bad	E-Mail and Phone required	Virtualization	Bad	No
OnionShare (preferred)	Yes	No	TBD[7]	TBD[7]	Yes (strong)	Yes	Good	Yes	Natively	Good	Yes (peer to peer)
Apple Messages (aka iMessage)	Yes	Closed-source[6]	No	Partial	No	No	Good	Apple device Required	Maybe Virtualization using real Apple device ID	Bad	No
IRC		No	No	No	No	Yes	Bad	Yes	Via Proxy[2] or Virtualization	Good	No
Jami (preferred)	Yes	No[373]	Yes	Yes	Partial	Yes	Good	Yes	Virtualization and only text[8]	Good	Partial
KakaoTalk (avoid)	Yes	Closed-source[6]	No[374]	No	No	No	Bad	No (but possible)	Virtualization	Bad	No
Keybase	Yes	No	Partial (exploding message)	No	No	Yes	Good	E-Mail Required			No
Kik (avoid)	No	Closed-source[6]	No	No	No	No	Bad	No (but possible)	Virtualization	Bad	No
Line (avoid)	Partial (opt-in)	Closed-source[6]	No	No	No	No	Bad	No (but possible)	Virtualization	Bad	No

[371] Briar Documentation, Bramble Transport Protocol version 4 https://code.briarproject.org/briar/briar-spec/blob/master/protocols/BTP.md [Archive.org]

[372] Serpentsec, Matrix https://serpentsec.1337.cx/matrix [Archive.org]

[373] Wikipedia, GnuTLS, https://en.wikipedia.org/wiki/GnuTLS [Wikiless] [Archive.org]

[374] KTH ROYAL INSTITUTE OF TECHNOLOGYSCHOOL OF ELECTRICAL ENGINEERING, A Security and Privacy Audit of KakaoTalk's End-to-End Encryption www.diva-portal.org/smash/get/diva2:1046438/FULLTEXT01.pdf [Archive.org]

Pidgin with OTR (avoid)	Yes (OTR [375])	No	Yes	No	No	Yes	Bad	Yes	Via Proxy[2] or Virtualization	Bad[376]	No
qTox	Yes	No	No	No	No	Yes	Good	Yes	Via Proxy[2] or Virtualization	Medium [377]	Yes
Session	Yes	No	No	Yes	Yes	Yes	Good	Yes	Natively	Good	Yes
Signal	Yes	No	Yes	Yes	Yes (moderate)	Yes	Good	Phone Required	Virtualization	Good	No
Skype (avoid)	Partial (Only 1to1 / opt-in)	Closed-source[6]	No	No	No	No	Bad	No (but possible)	Virtualization	Bad	No
SnapChat (avoid)	No	Closed-source[6]	No	No	No	No	Bad	No (but possible)	Virtualization	Bad	No
Teams (avoid)	Yes	Closed-source[6]	No	No	No	No	Bad	No (but possible)	Virtualization	Bad	No
Telegram	Partial (Only 1to1 / opt-in)	Yes (MTProto[378])	Partial (secret chats only)	Yes	No	Partial[4]	Medium (e2ee off by default)	Phone Required	Via Proxy[2] or Virtualization	Medium [379]	No
Viber (avoid)	Partial (Only 1to1)	Closed-source[6]	Yes	No	No	No	Bad	No (but possible)	Virtualization	Bad	No
WeChat (avoid)	No	Closed-source[6]	No	No	No	No	Bad	No	Virtualization	Bad	No
WhatsApp (avoid)	Yes	Closed-source[6]	Yes	No	No	No	Bad	Phone Required	Virtualization	Bad	No
Wickr Me	Partial (Only 1to1)	No	Yes	No	Yes (moderate)	No	Good	Yes	Virtualization	Good	No
Gajim (XMPP) (preferred)	Partial (Only 1to1)	No	Yes	No	No	Yes	Good	Yes	Via Proxy[2] or Virtualization	Good	Partial
Zoom (avoid[380])	Disputed[381]	No	TBD[7]	No	No	No	Bad	E-Mail Required	Virtualization	Bad[382]	No

Legend:

- 0, the mention "preferred" or "avoid" refers to the use of those apps for sensitive communications in my opinion. This is just my opinion and you can make your own using the resources above and others. Remember "Trust but verify".
- 1, e2ee = end to end encryption
- 2, Additional steps might be needed for securing Tor Connectivity
- 3, Their ability and willingness to fight for privacy and not cooperate with various adversaries
- 4, Only the client apps are open-source, not the server-side apps
- 5, This means the data is fully encrypted at rest (and not only during transit) and unreadable by any third party without a key you only know (including backups)
- 6, Unverifiable because it is proprietary closed-source.
- 7, To Be Determined, unknown at the time of this writing
- 8, Jami Media Protocol needs UDP at this time which is not supported by Tor (supports only TCP)

[375] Wikipedia, OTR https://en.wikipedia.org/wiki/Off-the-Record_Messaging [Wikiless] [Archive.org]

[376] Pidgin Security Advisories, https://www.pidgin.im/about/security/advisories/ [Archive.org]

[377] Whonix Forum, Tox Integration https://forums.whonix.org/t/tox-qtox-whonix-integration/1219 [Archive org]

[378]Telegram Documentation, MTProto Mobile Protocol https://core.telegram.org/mtproto [Archive.org]

[379] Wikipedia, Telegram Security Breaches, https://en.wikipedia.org/wiki/Telegram_(software)#Security_breaches [Wikiless] [Archive org]

[380] TechCrunch, Maybe we shouldn't use Zoom after all, https://techcrunch.com/2020/03/31/zoom-at-your-own-risk/ [Archive.org]

[381] The Incercept, Zoom Meetings Aren't End-to-End Encrypted, Despite Misleading Marketing https://theintercept.com/2020/03/31/zoom-meeting-encryption/ [Archive.org]

[382] Serpentsec, Secure Messaging: Choosing a chat app https://serpentsec.1337.cx/secure-messaging-choosing-a-chat-app [Archive org]

Some apps like Threema and Wire were excluded from this comparison due to not being free and not accepting anonymous cash methods such as Cash/Monero.

Conclusion:

I will recommend these options in that order (as also recommend by privacytools.io[383,384] except for Session):

- Native Tor Onion Routing Support (**preferred**):
  - Briar (https://briarproject.org/ [Archive.org])* **(Android/Linux only)**
  - OnionShare version >2.3 (https://onionshare.org/ [Archive.org])* **(Desktop multiplatform only)**
- Non-Native Tor Support (needs additional steps for ideal anonymity):
  - Jami (https://jami.net/ [Archive org])
  - Element/Matrix.org (https://element.io/ [Archive.org])

* Note that these options (Briar and OnionShare) do not support multi-devices yet. Your information is strictly stored on the device/OS where you are setting it up. Do not use those on a non-persistent OS unless you want ephemeral use.

Note that all the non-native Tor options must be used over Tor for safety (from Tails or a guest OS running behind the Whonix Gateway such as the Whonix Workstation or an Android-x86 VM).

While I do not recommend most of those platforms for the various reasons outlined above (phone number and e-mail), this does not mean it is not possible to use them anonymously if you know what you are doing. You can use even Facebook Messenger anonymously by taking the necessary precautions outlined in this guide (virtualization behind a Tor Gateway on a non-persistent OS).

The ones that are preferred are recommended due to their stance on privacy, their default settings, their crypto choices but also because they allow convenient anonymous sign-up without going through the many hassles of having a phone number/e-mail verification method and are open-source.

Those should be privileged in most cases. Yes, this guide has a discord server, and a twitter account despite those not being recommended at all for their stance on privacy and their struggle with anonymity. But this is about me acting appropriately in making this guide available to the many and conveniently using my experience and knowledge to do so as anonymously as possible.

I do not endorse or recommend some mainstream platforms for anonymity including the much-praised Signal which to this date still requires a phone number to register and contact others. In the context of this guide, I strongly recommend against using Signal if possible.

Redacting Documents/Pictures/Videos/Audio safely:

You might want to self-publish some information safely and anonymously in the form of writing, pictures, videos, …

For all these purposes here are a few recommendations:

- Ideally, you should not use proprietary software such as Adobe Photoshop, Microsoft Office…
- Preferably, you should use open-source software instead such as LibreOffice, Gimp…

While the commercial alternatives are feature rich, they are also proprietary closed-source and often have various issues such as:

- Sending telemetry information back to the company.
- Adding unnecessary metadata and sometimes watermarks to your documents.
- These apps are not free and any leak of any metadata could be traced back to you since you had to buy these somewhere.

[383] Privacytools.io, File-Sharing https://privacytools.io/software/file-sharing/ [Archive.org]

[384] Privacytools.io, Real-Time Communication https://privacytools.io/software/real-time-communication/ [Archive org]

It is possible to use commercial software for making sensitive documents but you should be extra-careful with all the options in the various Apps (commercia or free) to prevent any data leak from revealing information about you.

Here is a comparative table of recommended/included software compiled from various sources (Privacytools.io, Whonix, Tails, Prism-Break.org and myself). Keep in mind my recommendation considers the context of this guide with only sporadic online presence on a need basis.

Type	Whonix	Prism-Break.org	Privacytools.io	Tails	This guide
Offline Document Editing	LibreOffice	N/A	LibreOffice*	LibreOffice	LibreOffice; Notepad++
Online Document Editing (collaboration)	N/A	Cryptpad.fr	Cryptpad.fr; Etherpad.org; Privatebin.net	N/A	Cryptpad.fr; Etherpad.org; Privatebin.net
Pictures Editing	Flameshot (L)	N/A	N/A	GIMP	GIMP
Audio Editing	Audacity	N/A	N/A	Audacity	Audacity
Video Editing	Flowblade (L)	N/A	N/A	N/A	Flowblade (L) Olive (?) OpenShot (?) ShotCut (?)
Screen Recorder	Vokoscreen	N/A	N/A	N/A	Vokoscreen
Media Player	VLC	N/A	N/A	VLC	VLC
PDF Viewer	Ristretto (L)	N/A	N/A	N/A	Browser
PDF Redaction	PDF-Redact Tools (L)	N/A	N/A	PDF-Redact Tools (L)	LibreOffice; PDF-Redact Tools (L)

Legend: * Not recommended but mentioned. N/A = Not Included or absence of recommendation for that software type. (L)= Linux Only but can maybe be used on Windows/MacOS through other means (HomeBrew, Virtualization, Cygwin). (?)= Not tested but open-source and could be considered.

In all cases, I strongly recommend only using such applications from within a VM or Tails to prevent as much leaking as possible. If you do not, the you will have to sanitize those documents carefully before publishing (See Removing Metadata from Files/Documents/Pictures).

Communicating sensitive information to various known organizations:

You might be interested in communicating information to some organization such as the press anonymously.

If you must do so, you should take some steps because you cannot really trust any organization to protect your anonymity[385]:

- Check the files for any metadata: see Removing Metadata from Files/Documents/Pictures
- Check the files for anything malicious: see Appendix T: Checking files for malware
- Check the files for any watermarking: see Watermarking
- Assess carefully the potential consequences and risks of communicating any sensitive information for you and others (legally, ethically, and morally). Remember … Do not be evil. Legal is not necessarily Good.

After curating the files for anything you want to leave out. Double check and even Triple check them. Then you could consider sending them to an organization such as a press organization or others.

For this, I strongly recommend the use of SecureDrop[386] (https://securedrop.org/ [Archive.org]) which is an open-source project from the Freedom of the Press foundation.

[385] Praxis Films, Open Letter from Laura Poitras https://www.praxisfilms.org/open-letter-from-laura-poitras/ [Archive.org]

[386] Wikipedia, SecureDrop https://en.wikipedia.org/wiki/SecureDrop [Wikiless] [Archive org]

Ideally you should use SecureDrop over Tor and you will find a curated list of those here https://github.com/alecmuffett/real-world-onion-sites [Archive.org]

If not SecureDrop is not available, you could consider any other mean of communication but you should privilege those that are encrypted end to end. **Do not ever do this from your real identity but only from a secure environment using an anonymous identity.**

Without SecureDrop you could consider:

- Using e-mail with GPG encryption provided your recipient has published a GPG key somewhere. You can look this up here:
  - On their verified Social Media accounts (Twitter) if they provided it.
  - On https://keybase.io (Tor address http://keybase5wmilwokqirssclfnsqrjdsi7jdir5wy7y7iu3tanwmtp6oid.onion)
  - On open PGP directories such as: **(be careful as those are public directories and anyone can upload any key for any e-mail address, you will have to cross-check the signature with other platforms to be sure it is theirs).**
    - http://keys.gnupg.net/
    - https://pgp.mit.edu/
    - https://keyserver.ubuntu.com/
    - https://keys.openpgp.org
- Using any other platform (even Twitter DMs) but again using GPG to encrypt the message for the recipient.

What you should avoid IMHO:

- Do not send physical materials using the post due to the risk of leaving DNA/Fingerprints or other traceable information (see Cash-Paid VPN (preferred)).
- Do not use methods linked to a phone number (even a burner one) such as Signal/WhatsApp/Telegram.
- Do not use any kind of voice/video communication.
- Do not leak any clues about your real identity when exchanging messages.
- Do not meet people in real life unless you have absolutely no other option (this is a last resort).

If you intend to break your anonymity to protect your safety:

- Assess the risks very carefully first.
- Inform yourself carefully on the legality/safety of your intent and the consequences for you and others. Think about it carefully.
- Possibly reach out to a **trusted** lawyer before doing so.

Maintenance tasks:

- You should sign-up carefully into your accounts from time to time to keep them alive.
- Check your e-mail regularly for security checks and any other account notification.
- Check regularly the eventual appearance of compromise of any of your identities using https://haveibeenpwned.com/ [Archive.org] (obviously from a safe environment).

Backing-up your work securely:

Do not ever upload encrypted file containers with plausible deniability (hidden containers within them) to most cloud services (iCloud, Google Drive, OneDrive, Dropbox) without safety precautions. This is because most cloud services keep backups/versioning of your files and such backups/versioning of your encrypted containers can be used for differential analysis to prove the existence of a hidden container.

Instead, this guide will recommend other methods of backing up your stuff safely.

Offline Backups:

These backups can be done on an external hard drive or an USB key. Here are the various possibilities.

Selected Files Backups:

Requirements:

For these back-ups, you will need an USB key or an external hard drive with enough capacity to store the files you want to back-up.

Veracrypt:

For this purpose, I will recommend the use of Veracrypt on all platforms (Linux/Windows/MacOS) for convenience/security and portability.

Normal File containers:

The process is fairly simple and all you will need is to follow Veracrypt tutorial here: https://www.veracrypt.fr/en/Beginner%27s%20Tutorial.html [Archive.org]

In this container, you can then store sensitive data manually and or use any backup utility you want to backup files from the OS to that container.

You can then store this container anywhere safe.

Hidden File containers with plausible deniability:

The process is also fairly simple and similar to the previous tutorial except this time you will use the Veracrypt wizard to create a Hidden Veracrypt Volume instead of a Standard Veracrypt Volume.

You can create a Hidden volume within an existing Standard Volume or just use the wizard to create a new one.

Let us say you want a container of 8GB, the Wizard will first create an "outer volume" where you will be able to store decoy information when prompted. Some decoy files (somewhat sensible, plausible but what you really want to hide) should be stored in the decoy volume.

Then Veracrypt will ask you to create a smaller hidden container (for instance 2GB or 4GB) within the outer volume where you can store your actual hidden files.

When you select the file for mounting in Veracrypt, depending on which password you provide, it will mount the Outer decoy volume or the Hidden volume.

You can then mount your hidden volume and use it to store sensitive files normally.

Be careful when mounting the Outer decoy volume to update its content. You should protect the hidden volume from being overwritten when doing this as working in the decoy volume could overwrite data in the hidden volume.

To do this, when mounting the Decoy Volume, select Mount Options and Check the "Protect hidden volume" option and provide the hidden volume password on the same screen. Then mount the decoy volume. This will protect the hidden volume from being overwritten when changing the decoy files. This is also explained here in Veracrypt documentation: https://www.veracrypt.fr/en/Protection%20of%20Hidden%20Volumes.html [Archive.org]

Be extremely cautious with these file containers:

- **Do not store multiple versions of them or store them anywhere where some versioning is being done (by the file system or the storage system). These file containers should be identical everywhere you store them. If you have a backup of such containers somewhere, it needs to be absolutely identical to the one you are using. If you do not take this precaution, an adversary could compare two different versions of this container and prove the existence of hidden data. Follow carefully the recommendations here https://www.veracrypt.fr/en/Security%20Requirements%20for%20Hidden%20Volumes.html [Archive.org]. Remember the Local Data Leaks and Forensics: section.**
- I strongly recommend storing such containers on external USB keys that you will only mount from your guest VMs and never from your Host OS. **After each modification to the files, you should clean the free space on the USB disk and make sure that any backup of such containers is absolutely identical on each key and your computer. See the How to securely delete specific files/folders/data on your HDD/SSD and Thumb drives section of this guide for help on doing this.**

- If you have time, **I would even recommend you delete wipe the keys completely before making any modification on such containers on your computer (if you do not work from the USB key directly).** This is to prevent an adversary that would seize your assets before you could update the keys from having multiple versions of the containers that could lead to proving the existence of hidden data using forensics techniques.
- **Do not ever store such containers on cloud storage platforms that have backups and where you have no direct control over permanent deletion. They might keep "old versions" of your files which can then also be used by forensics to prove the existence of hidden data.**
- If you are mounting the hidden volume from your Host OS (**not recommended**), you should erase all traces of this hidden volume everywhere after use. There could be traces in various places (system logs, file systems journaling, recent documents in your applications, indexing, registry entries…). Refer to the Some additional measures against forensics section of this guide to remove such artifacts. Especially on Windows. Instead, you should mount them on your Guest VMs. With Virtualbox for instance, you could take a snapshot of the VM before opening/working the hidden volume and then restore the snapshot prior to opening/working on it after use. This should erase the traces of its presence and mitigate the issue. Your Host OS might keep logs of the USB key being inserted but not of the hidden volume usage. Therefore, I do not recommend using these from your host OS.
- Do not store these on external SSD drives if you are not sure you can use Trim on them (see the Understanding HDD vs SSD section).

Full Disk/System Backups:

TLDR version: Just use Clonezilla as it worked reliably and consistently with all my tests on all operating systems except for Macs where you should probably use native utilities (Time Machine/Disk utility instead) to avoid compatibility issues and since you are using Native MacOS encryption. When using Windows, do not backup a partition containing a hidden OS in case you use Plausible Deniability (as explained before, this backup could allow an adversary to prove the existence of the hidden OS by comparing the last backup to the current system where data will have changed and defeat plausible deniability, use file containers instead).

You will have two options here:

- (Not recommended) Doing your backup from the live operating system using a back-up utility (commercial utilities such as EaseUS Todo Free, Macrium Reflect…) or native utilities like MacOS Time Machine, QubesOS Backup, Ubuntu Déjà Dup or Windows Backup…).
    - This backup can be done while the Operating System is running.
    - This backup will not be encrypted using the disk encryption but using the Backup utility encryption algorithm (which you will have to trust and cannot really control for most). Alternatively, you could encrypt the backup media yourself separately (for instance with Veracrypt). I am not aware of any free or non-free utility that natively supports Veracrypt.
    - Some utilities will allow for differential/incremental backups instead of full backups.
    - These backup utilities will not be able to restore your encrypted drive as-is as they do not support those encrypted file systems natively. And so, these restore will require more work to restore your system in an encrypted state (re-encryption after restore).
- (Recommended) Doing it offline from a boot drive (such as with the free open-source Clonezilla).
    - This backup can only be done while the Operating System is not running.
    - This backup will back up the encrypted disk as-is and therefore will be encrypted by default with the same mechanism (it is more like a fire and forget solution). The restore will also restore the encryption as-is and your system will immediately be ready to use after a restore.
    - This method will not allow incremental/differential back-ups (meaning you will have to re-do a full back-up every time).
    - This method is clearly the easiest to manage.

I made extensive testing using live backups utilities (Macrium Reflect, EaseUS Todo Reflect, Déjà Dup…) and personally I do not think it is worth it. Instead, I would recommend that you periodically back-up your system with a simple Clonezilla image. It is much easier to perform, much easier to restore and usually works reliably without

issues in all cases. And contrary to many beliefs, it is not that slow with most backups taking about an hour depending on the speed of your destination media.

For backing up single files while you work, I recommend using file containers or encrypted media directly and manually as explained in the previous section.

Requirements:

You will need a separate external drive with at least the same or more free space available than your source disk. If your laptop has a 250GB disk. You will need at least 250GB of free disk space for the full image backup. Sometimes this will be reduced significantly with compression by the backup utility but as a safety rule you should have at least the same or more space on your backup drive.

Some general warnings and considerations:

- If you use Secure Boot, you will need a backup utility that supports Secure Boot which includes Clonezilla AMD64 versions.
- Consider the use of exFAT as file system for your backup drives as those will provide better compatibility between various OSes (MacOS, Linux, and Windows) vs NTFS/HFS/ext4...

Linux:

Ubuntu (or any other distro of choice):

I will recommend the use of the open-source Clonezilla utility for convenience and reliability but there are many other native Linux utilities and methods you could use for this purpose.

So, you should follow the steps in Appendix E: Clonezilla

QubesOS:

Qubes OS recommends using their own utility for backups as documented here https://www.qubes-os.org/doc/backup-restore/ [Archive.org] . But I think it is just a hassle and provides limited added value unless you just want to back-up a single Qube. So instead, I am also recommending just making a full image with Clonezilla which will remove all the hassle and bring you back a working system in a few easy steps.

So, you should follow the steps in Appendix E: Clonezilla

Windows:

I will only recommend the use of the open-source and free Clonezilla utility for this purpose. There are commercial utilities that offer the same functionality but I do not see any advantage in using any of them vs Clonezilla.

Some warnings:

- If you use Bitlocker for encryption with TPM[387] enabled, you might need to save your Bitlocker Key (safely) somewhere as well as this might be needed to restore your drive if your HDD/SSD or other hardware parts changed. Another option would be to use Bitlocker without the use of TPM which would not require this option. But again, I do not recommend using Bitlocker at all.
- You should always have a backup of your Veracrypt rescue disk at hand somewhere to able to resolve some issues that might still appear after a restore. Remember this rescue disk does not contain your passphrase or any sensitive information. You can store it as is.
- If you changed the HDD/SSD after a failure, it is possible that Windows 10 will refuse to boot if your hard drive ID changed. You should also save this ID prior to backing up as you might need to change the ID of the new drive as Windows 10 might require a matching ID before booting. See Appendix F: Diskpart
- **In case you are using Plausible Deniability on Windows. DO NOT back-up the hidden OS partition as this image could be used by Forensics to prove the existence of the hidden volume as explained earlier. It is okay to back-up the Decoy OS partition without issues but you should never backup the partition containing the Hidden OS.**

Follow the steps in Appendix E: Clonezilla

---

[387] Wikipedia, TPM https://en.wikipedia.org/wiki/Trusted_Platform_Module [Wikiless] [Archive.org]

MacOS:

I would recommend just using the native Time Machine backup with encryption (and a strong passphrase that could be the same as your OS) as per the guides provided at Apple: https://support.apple.com/en-ie/guide/mac-help/mh21241/mac [Archive.org] and https://support.apple.com/en-ie/guide/mac-help/mh11421/11.0/mac/11.0 [Archive org].

So, plug in an external drive and it should prompt you to use it as a Time Machine backup.

You should however consider formatting this drive as exFAT to that it is also usable by other OSes conveniently (Windows/Linux) without added software using this guide: https://support.apple.com/en-ie/guide/disk-utility/dskutl1010/mac [Archive org]

It is just simpler and will work online while you work. You will be able to recover your data on any other Mac from the recovery options and you will be also able to use this disk for backing up other devices.

It is possible to also use Clonezilla to clone your Mac Hard Drive but it could bring hardware compatibility issues and probably will not add much in terms of security. So, for MacOS I am not specifically recommending Clonezilla.

Online Backups:

Files:

This is a tricky one. The problem is that it depends on your threat model.

- **TLDR: Do not store file containers with plausible deniability (Veracrypt) online.** If you use containers with plausible deniability, you should never ever store them on any platform where you do not have full control over the deletion process as the platform will most likely have backups of previous versions for some time. And again, these previous versions could allow forensics to prove the existence of hidden data and defeat plausible deniability. This includes platforms like DropBox, Google Drive, OneDrive, or others. The only acceptable online storage of those could be "cold storage" (meaning you will never change those files again and just keep them away untouched compared to any local version).
- If you use normal encrypted backups without plausible deniability, you could store them pretty much anywhere if they are properly encrypted locally before uploading (for example with Veracrypt, using strong passphrases and encryption). **Do not ever trust encryption of any online provider. Only trust your own local encryption (using Veracrypt for instance).** For these cases, you could store your backups pretty much anywhere in the accounts of your online identities (iCloud, Google Drive, DropBox…) if they are strongly encrypted locally before uploading. But you could also prefer privacy caring services such as Cryptpad.fr (1GB).

Obviously do not ever do/access those backups from unsecure/unsafe devices but only from the secure environments you picked before.

Self-hosting:

Self-hosting (using Nextcloud for instance) is also a possibility provided you do have an anonymous hosting

Please see Appendix A1: Recommended VPS hosting providers.

Please also consider this Monero Disclaimer.

Cloud-hosting:

For smaller files, consider Cryptpad.fr as recommended by Privacytools.io at https://privacytools.io/providers/cloud-storage/ [Archive.org] (limited to 1GB total).

I am currently not aware of any online storage/hosting platform accepting cash payments unlike providers mentioned before.

If you do intend to store sensitive data on "mainstream platforms" (Dropbox, Google Drive, OneDrive…), remember not to ever store plausible deniability containers on those and remember to encrypt anything locally before uploading there. Either with a software like Veracrypt or with a software like Cryptomator

(https://cryptomator.org/). Do not ever upload non-encrypted files on those platforms and repeating myself, only access them from a secure shielded VM.

Information:

If you just want to save information (text), I will recommend the use secure and private pastebins[388]. Mostly I will stick to the ones recommended by privacytools.io (https://privacytools.io/providers/paste/ [Archive.org]):

- https://privatebin.info/
- https://cryptpad.fr/pad/

On these providers you can just create a password protected pad with the information you want to store.

Just create a pad, protect it with a password and write your info in it. Remember the address of the pad.

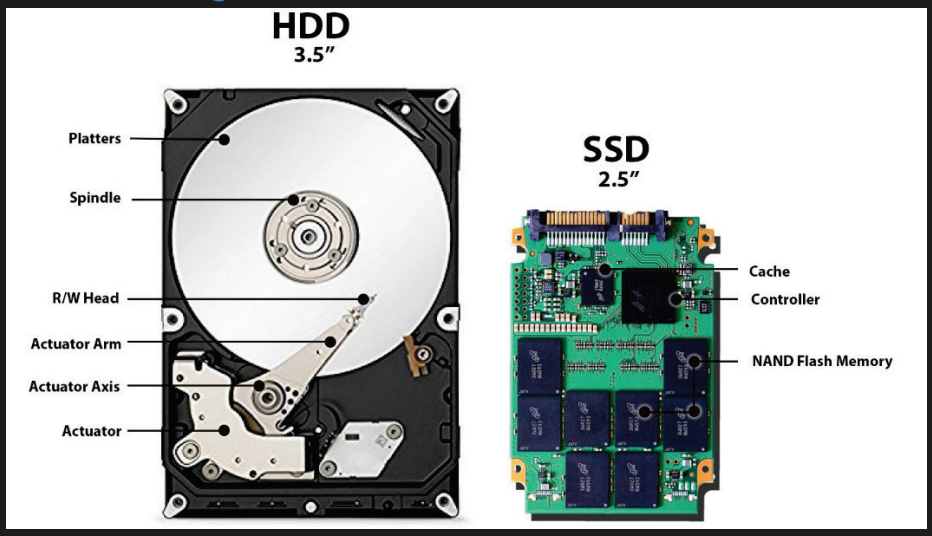
Synchronizing your files between devices Online:

To that the answer is very simple and a clear consensus for everyone: https://syncthing.net/ [Archive.org]

Just use SyncThing, it is the safest and most secure way to synchronize between devices, it is free and open-source, and it can easily be used in a portable way without install from a container that needs syncing.

Covering your tracks:

Understanding HDD vs SSD:



If you intend to wipe your whole HDD laptop, the process is rather simple and straightforward. The data is written at a precise location on a magnetic (hard) platter (why it is called a hard drive) and your OS knows precisely where it is on the platter, where to delete it and where to overwrite it for secure deletion using simple processes (like just overwriting that location over and over until no traces are left).

On the other hand, if you are using an SSD drive, the process is not as simple as the drive uses several internal mechanisms to extent its lifespan and performance. Three of those processes are of particular interest when it comes to us in this guide. SSD drives are divided themselves into 2 main categories:

- ATA Drives (usually SATA and usually 2.5" format as the image above).
- NVMe Drives (usually M.2 format as the illustration below).

Here are examples of the most common formats:

[388] Wikipedia, Pastebin https://en.wikipedia.org/wiki/Pastebin [Wikiless] [Archive.org]

All of these are sold as internal and external drives within enclosures.

The methods and utilities to manage/wipe them will vary depending on the type of drive you are using. So, it is important you know which one you have within your laptop.

On most recent laptops, chances are high that it will be one of the middle options (M.2 SATA or M.2 NVMe).

Wear-Leveling.

These drives use a technique called wear leveling[389]. At a high level, wear leveling works as follows. The space on every disk is divided into blocks that are themselves divided into pages, kind of like the chapters in a book are made of pages. When a file is written to disk, it is assigned to a certain set of pages and blocks. If you wanted to overwrite the file in an HDD, then all you would have to do is tell the disk to overwrite those blocks. But in SSDs and USB drives, erasing and re-writing the same block can wear it out. Each block can only be erased and rewritten a limited number of times before that block just will not work anymore (the same way if you keep writing and erasing with a pencil and paper, eventually the paper might rip and be useless). To counteract this, SSDs and USB drives will try to make sure that the number of times each block has been erased and rewritten is about the same, so that the drive will last as long as possible (thus the term wear leveling). As a side effect, sometimes instead of erasing and writing the block a file was originally stored on, the drive will instead leave that block alone, mark it as invalid, and just write the modified file to a different block. This is kind of like leaving the chapter in the book unchanged, writing the modified file on a different page, and then just updating the book's table of contents to point to the new location. All of this occurs at a very low level in the electronics of the disk, so the operating system does not even realize it has happened. This means, however, that even if you try to overwrite a file, there is no guarantee the drive will actually overwrite it, and that's why secure deletion with SSDs is so much harder.

Wear-leveling alone can therefore be a disadvantage for security and an advantage for adversaries such as forensics examiners. This feature makes classic "secure deletion" counter-productive and useless and is why this feature was removed on some Operating Systems like MacOS (a as from version 10.11 El Capitan) where you could enable it before on the Recycle Bin.

Most of those old secure deletion utilities were written with HDD in mind and have no control over wear-leveling and are completely pointless when using an SSD. Avoid them on an SSD drive.

Trim Operations:

So, what now? Well here come the Trim[295, 390] operation. When you delete data on your SSD, your OS should support what is called a Trim operation command and **could (should)** issue this Trim command to the SSD drive periodically (daily, weekly, monthly…). This Trim command will then let know the SSD drive controller that there are pages within blocks containing data which are now free to be really deleted without deleting anything itself.

---

[389] Wikipedia, Wear Leveling https://en.wikipedia.org/wiki/Wear_leveling [Wikiless] [Archive.org]

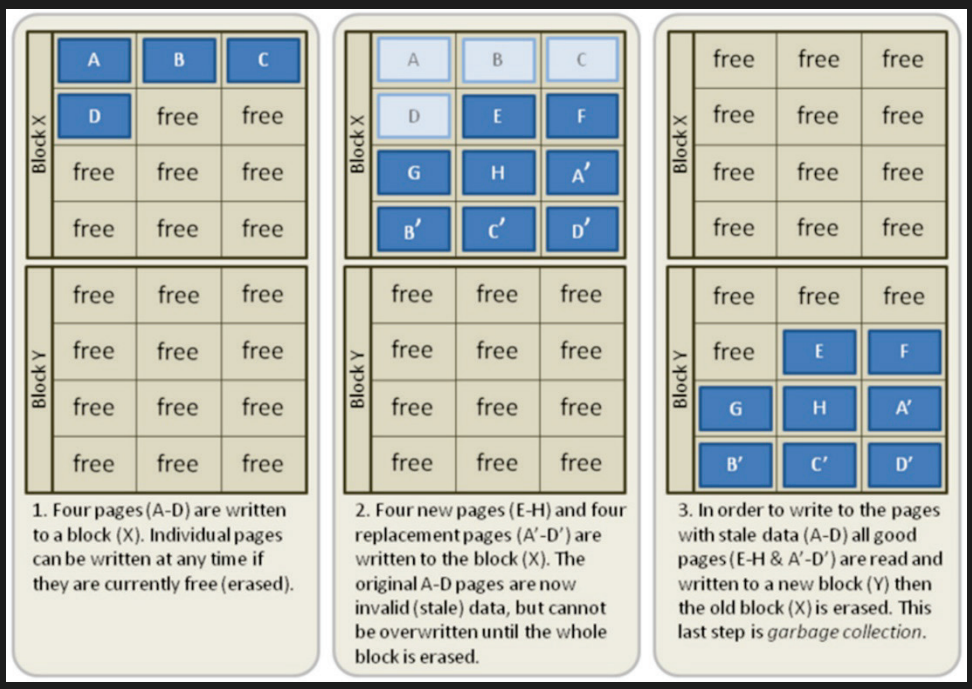
[390] Wikipedia, Trim https://en.wikipedia.org/wiki/Write_amplification#TRIM [Wikiless] [Archive.org]

Trim should be enabled by default on all modern Operating Systems detecting an SSD drive covered in this guide (MacOS, Windows 10, Ubuntu, Qubes OS…).

If Trim operations are not done regularly (or at all), then the data is never deleted pro-actively and at some point, all the blocks and pages will be occupied by data. Your OS will not see this and will just see free space as you delete files but your SSD controller will not (this is called Write Amplification[391]). This will then force the SSD controller to erase those pages and blocks on the fly which will reduce the write performance. This is because while your OS/SSD can write data to any free page in any bock, erasure is only possible on entire blocks therefore forcing your SSD to perform many operations to write new data. Overwriting is just not possible. This will defeat the wear-leveling system and cause performance degradation off SSD over time. Every time you delete a file on an SSD, your OS should issue a Trim command along with the deletion to let the SSD controller know the pages containing the file data are now free for deletion.

So, Trim itself does not delete any data but just marks it for deletion. Data deleted without using Trim (if Trim has been disabled/blocked/delayed for instance) will still be deleted at some point by the SSD garbage collection or if you want to overwrite what the OS sees at free space. But it might stick around for a bit longer than if you use Trim.

Here is an illustration from Wikipedia showing how it works on an SSD drive:



As you can see in the above illustration, data (from a file) will be written to the 4 first pages of Block X. Later new data will be written to the remaining pages and the data from the first files will be marked as invalid (for instance by a Trim operation when deleting a file). As explained on https://en.wikipedia.org/wiki/Trim_(computing) [Wikiless] [Archive org]; the erase operation can only be done on entire blocks (and not on single pages).

In addition to marking files for deletion (on reputable SSD drives) Trim usually makes those unreadable using a method called "Deterministic Read After Trim" or "Deterministic Zeroes After Trim". This means that if an adversary tries to read data from a trimmed page/block and somehow manages to disable garbage collection, the controller will not return any meaningful data.

Trim is your ally and should always be enabled when using an SSD drive and should offer sufficient reasonable protection. And this is also the reason you should not use Veracrypt Plausible deniability on a Trim enabled SSD as this feature is incompatible with Trim[392].

[391] Wikipedia, Write Amplification https://en.wikipedia.org/wiki/Write_amplification [Wikiless] [Archive.org]

[392] Wikipedia, Trim Disadvantages https://en.wikipedia.org/wiki/Trim_(computing)#Disadvantages [Wikiless] [Archive.org]

Garbage Collection:

Garbage collection[393] is an internal process running within your SSD drive that looks for data marked for erasure. This process is done by the SSD controller and you have no control over it. If you go back to the illustration above, you will see that Garbage collection is the last step and will notice that some pages are marked for deletion in a specific block, then copy the valid pages (not marked for deletion) to a different free destination block and then will be able to erase the source block entirely.

Garbage collection in itself does NOT require Trim to function but it will much faster and more efficient if Trim is performed. Garbage collection is one of the processes that will actually erase data from your SSD drive permanently.

Conclusion:

So, the fact is that it is very unlikely[394, 395] and difficult for a forensic examiner to be able to recover data from a Trimmed SSD but it is not completely impossible either[396, 397, 398] if they are fast enough and have access to extensive equipment, skills and motivation.

Within the context of this guide which also uses full disk encryption. Deletion and Trim should be reasonably enough on any SSD drive and will be recommended as the standard method of deletion.

How to securely wipe your whole Laptop/Drives if you want to erase everything:

So, you want to be sure. To achieve 100% secure deletion on an SSD drive, we will need to use specific SSD techniques (If you are using an HDD drive, skip this part and go to your OS of choice):

- Easy options for less experienced users:
  - If available, just use the Secure Erase option available from your BIOS/UEFI (ATA/NVME Secure Erase or Sanitize).

---

[393] Wikipedia, Garbage Collection https://en.wikipedia.org/wiki/Write_amplification#Garbage_collection [Wikiless] [Archive.org]
[394] Techgage, Too TRIM? When SSD Data Recovery is Impossible https://techgage.com/article/too_trim_when_ssd_data_recovery_is_impossible/ [Archive.org]
[395] ResearchGate, Live forensics method for acquisition on the Solid-State Drive (SSD) NVMe TRIM function https://www.researchgate.net/publication/341761017_Live_forensics_method_for_acquisition_on_the_Solid_State_Drive_SSD_NVMe_TRIM_function [Archive org]
[396] ElcomSoft, Life after Trim: Using Factory Access Mode for Imaging SSD Drives https://blog.elcomsoft.com/2019/01/life-after-trim-using-factory-access-mode-for-imaging-ssd-drives/ [Archive.org]
[397] Forensic Focus, Forensic Acquisition Of Solid State Drives With Open Source Tools https://www.forensicfocus.com/articles/forensic-acquisition-of-solid-state-drives-with-open-source-tools/ [Archive.org]
[398] ResearchGate, Solid State Drive Forensics: Where Do We Stand? https://www.researchgate.net/publication/325976653_Solid_State_Drive_Forensics_Where_Do_We_Stand [Archive.org]

    - Just re-install a fresh operating system (delete/quick format the drive) and re-encrypt it. The full disk encryption process should erase all previous data from the disk.
    - Buy PartedMagic[399] for 11$ and use it to erase any disk.
- Technical options for more advanced users:
    - ATA/NVMe Secure Erase: This method will remove the mapping table that keeps track of allocated data on the storage Blocks but does not destroy the actual data.
    - ATA/NVMe Sanitize Crypto Scramble (aka Instant Secure Erase, Crypto Erase), which applies to self-encrypting SSD drives: This method will change the encryption key of the self-encrypting SSD drive and render all the data stored in it unreadable.
    - ATA/NVMe Sanitize Block Erase: This method performs an actual block erase on every storage block and will destroy the data and change the encryption key if present.
    - ATA/NVMe Sanitize Overwrite **(very slow, could be dangerous and not recommended)**: This method performs a block erase and then overwrite every storage block (it is the same as Block Erase but will overwrite data in addition). This method is overkill and not necessary IMHO.

For maximum overkill paranoia security, Sanitize Block Erase option should be preferred but Secure Erase is probably more than enough when considering your drive is already encrypted. Unfortunately, are no **free** easy (bootable with a graphical menu) all-in-one tools available and you will be left with either going with drive manufacturers provided tools, the free manual hdparm[400] and nvme-cli[401] utilities or going with a commercial tool such as PartedMagic.

This guide will therefore recommend the use of the free utilities hdparm and nvme-cli using a Live System Rescue system.

If you can afford it, just buy Parted Magic for 11$ which provides an easy-to-use graphical tool for wiping SSD drives using the option of your choice[402, 403].

Note: Again, before proceeding, you should check your BIOS as some will offer a built-in tool to securely erase your drive (ATA/NVMe Secure Erase or ATA/NVMe Sanitize). If this is available, you should use that and the following steps will not be necessary. Check this before proceeding to avoid the hassle, see Appendix M: BIOS/UEFI options to wipe disks in various Brands).

Linux (all versions including Qubes OS):

System/Internal SSD:

- Option A: Check if your BIOS/UEFI has a built-in option to do so and if it does, use the correct option ("ATA/NVMe Secure Erase" or "ATA/NVMe Sanitize"). Do not use wipe with passes on an SSD drive.
- Option B: See Appendix D: Using System Rescue to securely wipe an SSD drive.
- Option C: Wipe your disk and re-install Linux with a new full disk encryption to overwrite all sectors with new encrypted data. **This method will be very slow compared to Option A and B as it will slowly overwrite your whole SSD. Also note that this might not be the default behavior when using LUKS. You might have to check the option to also encrypt the empty space for this effectively wipe the drive.**

Keep in mind all these options need to be applied on the entire physical drive and not on a specific partition/volume. If you do not, wear-leveling mechanisms might prevent this from working properly.

External SSD:

First please see Appendix K: Considerations for using external SSD drives

Trim should be sufficient in most cases and you could just use the blkdiscard command to force an entire device trim as explained here: https://wiki.archlinux.org/index.php/Solid_state_drive#Trim_an_entire_device [Archive.org]

---

[399] Wikipedia, Parted Magic https://en.wikipedia.org/wiki/Parted_Magic [Wikiless] [Archive.org]

[400] Wikipedia, hdparm https://en.wikipedia.org/wiki/Hdparm [Wikiless] [Archive.org]

[401] GitHub, nvme-cli https://github.com/linux-nvme/nvme-cli [Archive.org]

[402] PartedMagic Secure Erase, https://partedmagic.com/secure-erase/ [Archive org]

[403] Partedmagic NVMe Secure Erase, https://partedmagic.com/nvme-secure-erase/ [Archive.org]

If your USB controller and USB SSD disk supports Trim and ATA/NVMe secure erase, you could wipe them cautiously using hdparm using the same method as the System Disk above except you will not install Linux on it obviously. Keep in mind tho that this is not recommended (see Considerations above).

If it does not support Trim and/or ATA secure erase, you could (not securely) wipe the drive normally (without passes like an HDD) and re-encrypt it completely using your utility of choice (LUKS or Veracrypt for instance). The full disk decryption and re-encryption process will overwrite the entirety of the SSD disk and should ensure a secure wipe.

Alternatively, you could also (not securely) wipe the disk normally and then fill it completely with pseudorandom data which should also ensure secure deletion (this can be done with BleachBit https://www.bleachbit.org/download/linux [Archive org] or from the command line using secure-delete using this tutorial https://superuser.com/questions/19326/how-to-wipe-free-disk-space-in-linux [Archive.org]).

Keep in mind all these options need to be applied on the entire physical drive and not on a specific partition/volume. If you do not, wear-leveling mechanisms might prevent this from working properly.

Internal/System HDD:

- Option A: Check if your BIOS/UEFI has a built-in option and use them and if it does, use the correct option (Wipe + Passes in the case of an HDD).
- Option B: See Appendix I: Using ShredOS to securely wipe an HDD drive
- Option C: Wipe your disk and re-install Linux with a new full disk encryption to overwrite all sectors with new encrypted data. **This method will be very slow compared to Option A and B as it will slowly overwrite your whole HDD.**

External/Secondary HDD and Thumb Drives:

- Option A: Follow one of these tutorials:
  - https://linuxhint.com/completely_wipe_hard_drive_ubuntu/ [Archive.org]
  - https://linoxide.com/linux-command/commands-wipe-disk-linux/ [Archive.org]
  - https://wiki.archlinux.org/index.php/Securely_wipe_disk [Archive.org]

  I recommend using dd or shred for this purpose.

- Option B: Install and use BleachBit https://www.bleachbit.org/download/linux [Archive.org] or follow this EFF tutorial https://ssd.eff.org/en/module/how-delete-your-data-securely-linux [Archive.org]
- Option C: See Appendix I: Using ShredOS to securely wipe an HDD drive

Windows:

Unfortunately, you will not be able to wipe your Host OS using the Microsoft built-in tools within the settings. This is because your bootloader was modified with Veracrypt and will make the operation fail. In addition, this method would not be effective with an SSD drive.

System/Internal SSD:

- Option A: Check if your BIOS/UEFI has a built-in option to do so and if it does, use the correct option ("ATA/NVMe Secure Erase" or "ATA/NVMe Sanitize"). Do not use wipe with passes on an SSD drive.
- Option B: Check Appendix J: Manufacturer tools for Wiping HDD and SSD drives.
- Option C: See Appendix D: Using System Rescue to securely wipe an SSD drive.
- Option D: Wipe your disk and re-install Windows before performing a new full disk encryption (using Veracrypt or Bitlocker) to overwrite all sectors with new encrypted data. **This method will be slower compared to Option A and B as it will overwrite your whole SSD.**

Keep in mind all these options need to be applied on the entire physical drive and not on a specific partition/volume. If you do not, wear-leveling mechanisms might prevent this from working properly.

External SSD:

First please see Appendix K: Considerations for using external SSD drives

Use the manufacturer provided tools if possible. Those tools should provide support for safe secure erase or sanitize over USB and are available for most brands: See Appendix J: Manufacturer tools for Wiping HDD and SSD drives.

If you are not sure about the Trim support on your USB disk, (not securely) wipe it normally (simple quick format will do) and then encrypt the disk again using Veracrypt or alternatively Bitlocker. The full disk decryption and re-encryption process will overwrite the entirety of the SSD disk and should ensure a secure wipe.

Alternatively, you could also (not securely) wipe the disk normally and then fill it completely with pseudorandom data which should also ensure secure deletion (this can be done with BleachBit or PrivaZer free space erase options). See Extra Tools Cleaning.

Keep in mind all these options need to be applied on the entire physical drive and not on a specific partition/volume. If you do not, wear-leveling mechanisms might prevent this from working properly.

Internal/System HDD:

- Option A: Check if your BIOS/UEFI has a built-in option to do so and if it does, use the correct option (Wipe + Passes).
- Option B: Check Appendix J: Manufacturer tools for Wiping HDD and SSD drives
- Option C: See Appendix I: Using ShredOS to securely wipe an HDD drive

External/Secondary HDD and Thumb Drives:

- Option A: Check Appendix J: Manufacturer tools for Wiping HDD and SSD drives
- Option B: Use external tools such as:
  - Eraser (open-source): https://eraser.heidi.ie/download/ [Archive.org]
  - KillDisk Free: http://killdisk.com/killdisk-freeware.htm [Archive.org]
- Option C: See Appendix I: Using ShredOS to securely wipe an HDD drive

MacOS:

System/Internal SSD:

Unfortunately, the MacOS Recovery disk utility will not be able to perform a secure erase of your SSD drive as stated in Apple documentation https://support.apple.com/en-gb/guide/disk-utility/dskutl14079/mac [Archive.org].

In most cases, if your disk was encrypted with Filevault and you just perform a normal erase, it should be "enough" according to them. It is not according to me so you have no option besides re-installing MacOS again and re-encrypt it with Filevault again after re-installing. This should perform a "crypto erase" by overwriting your previous install and encryption. This method will be quite slow unfortunately.

If you want to do a faster secure erase (or have no time to perform a re-install and re-encryption), you can try using the method described in Appendix D: Using System Rescue to securely wipe an SSD drive.**(This will not work on M1 Macs)**. **Be careful tho as this will also erase your recovery partition which is needed to reinstall MacOS.**

External SSD:

First please see Appendix K: Considerations for using external SSD drives

If your USB controller and USB SSD disk supports Trim and ATA secure erase, and if Trim is enabled on the disk by MacOS, you can just wipe the whole disk normally and data should not be recoverable on recent disks.

If you are not sure about Trim support or want more certainty, you can (not securely) wipe it using MacOS disk utility before fully re-encrypting them again using these two tutorials from Apple:

- https://support.apple.com/guide/disk-utility/erase-and-reformat-a-storage-device-dskutl14079/mac [Archive org]
- https://support.apple.com/guide/disk-utility/encrypt-protect-a-storage-device-password-dskutl35612/mac [Archive org] or using Veracrypt full disk encryption.

The full disk re-encryption process will overwrite the entirety of the SSD disk and should ensure a secure wipe.

Keep in mind all these options need to be applied on the entire physical drive and not on a specific partition/volume. If you do not, wear-leveling mechanisms might prevent this from working properly.

External HDD and Thumb Drives:

Follow this tutorial: https://support.apple.com/guide/disk-utility/erase-and-reformat-a-storage-device-dskutl14079/mac [Archive.org] and use the secure erase option from Disk Utility which should work fine on HDD and Thumb drives.

How to securely delete specific files/folders/data on your HDD/SSD and Thumb drives:

The same principles from the previous chapters apply to this one. The same issues arise too.

With an HDD drive, you can securely delete files by just deleting it and then apply one of more "passes" to overwrite the data in question. This can be done with many utilities on all OSes.

With an SSD drive however, again everything becomes a bit complicated because you are never sure anything is really deleted due to wear leveling, reliance on the Trim operation and garbage collection of the drive. An adversary that has the decryption key of your SSD (whether it is LUKS, Filevault 2, Veracrypt or Bitlocker) could unlock your drive and then attempt recovery using classic recovery utilities[404] and could succeed if the data was not trimmed properly. But this is again highly unlikely.

Since the Trim operation is not continuous on most recent hard drive but scheduled, simply forcing a Trim operation should be enough. But again, the only way to be 100% sure a file is securely deleted from your unlocked encrypted SSD is to again overwrite all the free space after deletion of the files in question or to decrypt/re-encrypt the drive. But I think this is overkill and not necessary. A simple disk wide Trim should be sufficient.

Remember tho that no matter the deletion method you use for any file on any medium (HDD drive, SSD, USB Thumb drive). It will probably leave other traces (logs, indexing, shellbags …) within your system and those traces will also need to be cleaned. Also remember that your drives should be fully encrypted and so this is most likely an extra measure. More on that later in the Some additional measures against forensics section.

Windows:

Remember you cannot use Trim at all if you are using Plausible Deniability on an SSD drive against all recommendations.

System/Internal SSD drive:

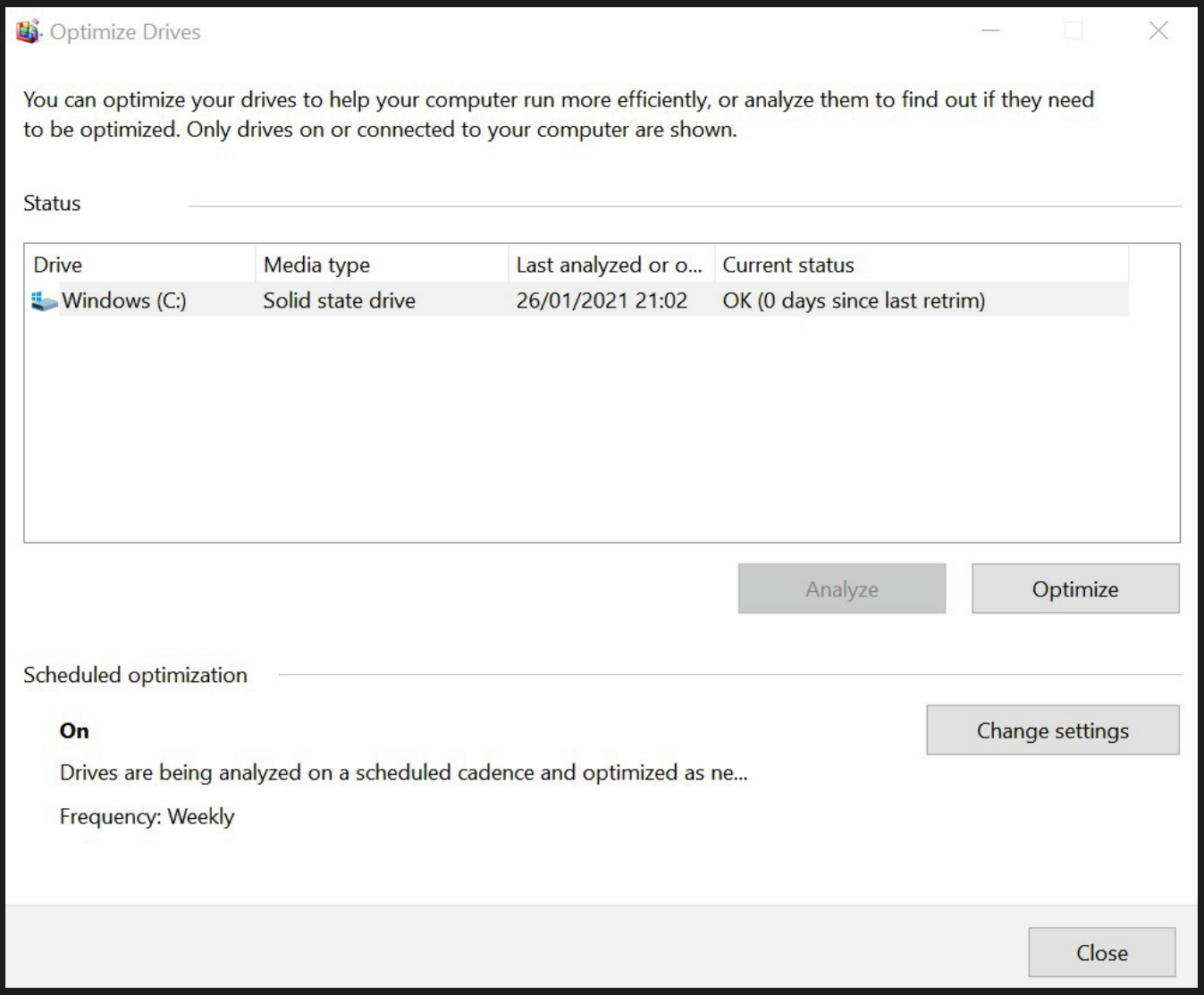
At this stage, and just delete the file permanently (empty the recycle bin) and trim/garbage collection will do the rest. This should be sufficient.

If you do not want to wait for the periodic Trim (set to Weekly by default in Windows 10), you could also force a disk wide Trim using the Windows native Optimize tool (see Appendix H: Windows Cleaning Tools).

If data was deleted by some utility (for instance by Virtualbox when reverting a snapshot), you could also issue a disk wide Trim to clean anything remaining using the same Optimize tool.

Just open Windows Explorer, Right Click on your System Drive and click Properties. Select Tools. Click Optimize and then Optimize again to force a Trim. You are done. I think that is probably enough in my opinion.

[404] UFSExplorer, Can I recover data from an encrypted storage? https://www.ufsexplorer.com/solutions/data-recovery-on-encrypted-storage.php [Archive.org]



If you want more security and do not trust the Trim operation then you will have no option but to either:

- Decrypt and re-encrypt (using Veracrypt or Bitlocker) the whole drive to overwrite all free space after data deletion. This will ensure overwriting of all the free space.
- Trim and then fill up the entire free space of the disk using a utility such as BleachBit or PrivaZer.

Keep in mind all these options need to be applied on the entire physical drive and not on a specific partition/volume. If you do not, wear-leveling mechanisms might prevent this from working properly.

Internal/External HDD or a USB Thumb Drive:

Please refer to Appendix H: Windows Cleaning Tools and pick a utility before proceeding.

The process is very simple depending on the tool you picked from the Appendix:

- Right Click a file/folder:
  - PrivaZer: Delete without a trace
  - BleachBit: Shred with BleachBit (or see this tutorial from the EFF https://ssd.eff.org/en/module/how-delete-your-data-securely-windows [Archive.org])

In the case of USB thumb drives, consider wiping free space using one of the above utilities after file deletion or wiping them completely using Eraser / KillDisk as instructed previously.

External SSD drive:

First please see Appendix K: Considerations for using external SSD drives

If Trim is supported and enabled by Windows for your external SSD drive. There should be no issue in securely deleting data normally just with normal delete commands. Additionally, you could also force a Trim using the Windows native Optimize tool (see Appendix H: Windows Cleaning Tools):

Just open Windows Explorer, Right Click on your System Drive and click Properties. Select Tools. Click Optimize and then Optimize again to force a Trim. You are done. I think that is probably enough in my opinion.

If Trim is not supported or you are not sure, you might have to ensure secure data deletion by:

- Filling up all the free space after any deletion (using BleachBit or PrivaZer for instance).
- Decrypt and Re-encrypt the disk with a different key after each deletion (using Veracrypt or Bitlocker).

Keep in mind all these options need to be applied on the entire physical drive and not on a specific partition/volume. If you do not, wear-leveling mechanisms might prevent this from working properly.

Linux (non Qubes OS):

System/Internal SSD drive:

Just permanently delete the file (and empty recycle bin) and it should be unrecoverable due to Trim operations and garbage collection.

If you do not want to wait for the periodic Trim (set to Weekly by default in Ubuntu), you could also force a disk wide Trim by running ```fstrim --all``` from a terminal. This will issue an immediate trim and should ensure sufficient security. This utility is part of the ```util-linux``` package on Debian/Ubuntu and should be installed by default on Fedora.

If you want more security and do not trust the Trim operation then you will have no option but to either:

- Decrypt and re-encrypt (using LUKS for instance following this tutorial https://wiki.archlinux.org/index.php/dm-crypt/Device_encryption#Re-encrypting_devices [Archive.org]) the whole drive to overwrite all free space after data deletion. This will ensure overwriting of all the free space.
- Trim using ```fstrim --all``` and then fill up the entire free space of the disk using a utility such as:
    - BleachBit https://www.bleachbit.org/download/linux [Archive.org]
    - Install secure-delete package and use sfill on the root of the drive:
        - ```sudo sfill -l -l /``` for instance should do the trick (this will take a substantial amount of time)
    - Use the old school dd method (taken from this answer https://superuser.com/questions/19326/how-to-wipe-free-disk-space-in-linux [Archive.org]) run these commands on the drive you want to fill:
        - ```dd if=/dev/zero of=zero.small.file bs=1024 count=102400```
        - ```dd if=/dev/zero of=zero.file bs=1024```
        - ```sync ; sleep 60 ; sync```
        - ```rm zero.small.file```
        - ```rm zero.file```

Keep in mind all these options need to be applied on the entire physical drive and not on a specific partition/volume. If you do not, wear-leveling mechanisms might prevent this from working properly.

Internal/External HDD drive or a Thumb Drive:

- You can do this the graphical way with BleachBit following this tutorial from the EFF: https://ssd.eff.org/en/module/how-delete-your-data-securely-linux [Archive.org]
- Or you can do this from the command line following this tutorial: https://linuxhint.com/completely_wipe_hard_drive_ubuntu/ [Archive.org] (For this purpose I recommend wipe and shred).

External SSD drive:

First please see Appendix K: Considerations for using external SSD drives

If Trim is supported and enabled by your Linux Distribution for your external SSD drive. There should be no issue in securely deleting data normally and just issue an ```fstrim --all``` from terminal to trim the drive. This utility is part of the "util-linux" package on Debian/Ubuntu and should be installed by default on Fedora.

If Trim is not supported or you want to be sure, you might have to ensure secure data deletion by filling up the entire free space of the disk using a utility such as:

- Decrypt and re-encrypt (using LUKS using this tutorial https://wiki.archlinux.org/index.php/dm-crypt/Device_encryption#Re-encrypting_devices [Archive.org] or Veracrypt from the graphical interface for instance) the whole drive to overwrite all free space after data deletion. This will ensure overwriting of all the free space.
- Fill the free space using one of those methods:
    - BleachBit https://www.bleachbit.org/download/linux [Archive.org]
    - Install secure-delete package and use sfill on the root of the drive:
        - ```sudo sfill -l -l /``` for instance should do the trick (this will take a substantial amount of time)
    - Use the old school dd method (taken from this answer https://superuser.com/questions/19326/how-to-wipe-free-disk-space-in-linux [Archive.org]) run these commands:
        - ```dd if=/dev/zero of=zero.small.file bs=1024 count=102400```
        - ```dd if=/dev/zero of=zero.file bs=1024```
        - ```sync ; sleep 60 ; sync```
        - ```rm zero.small.file```
        - ```rm zero.file```

Keep in mind all these options need to be applied on the entire physical drive and not on a specific partition/volume. If you do not, wear-leveling mechanisms might prevent this from working properly.

Linux (Qubes OS):

System/Internal SSD drive:

As with other Linux distros, normal deletion and trim should be sufficient on most SSD drives. So just permanently delete the file (and empty any recycle bin) and it should be unrecoverable due to periodic Trim operations and garbage collection.

Please follow this documentation to Trim within Qubes OS: https://github.com/Qubes-Community/Contents/blob/master/docs/configuration/disk-trim.md [Archive.org]

As with other Linux Systems, if you want more security and do not trust the Trim operation then you will have no option but to either:

- Decrypt and re-encrypt the whole drive to overwrite all free space after data deletion. This will ensure overwriting of all the free space. I didn't find a reliable tutorial on how to do this safely on Qubes OS but it's possible this Tutorial could work as well https://wiki.archlinux.org/index.php/dm-crypt/Device_encryption#Re-encrypting_devices [Archive.org] (at your own risk, this has not been tested yet).
- Refer to this Documentation (https://github.com/Qubes-Community/Contents/blob/master/docs/configuration/disk-trim.md [Archive.org]) and then trim using "fstrim --all" and then fill up the entire free space of the disk using an utility such as:
    - BleachBit https://www.bleachbit.org/download/linux [Archive.org]
    - Install secure-delete package and use sfill on the root of the drive:
        - ```sudo sfill -l -l /``` for instance should do the trick (this will take a substantial amount of time)
    - Use the old school dd method (taken from this answer https://superuser.com/questions/19326/how-to-wipe-free-disk-space-in-linux [Archive.org]) run these commands on the drive you want to fill:
        - ```dd if=/dev/zero of=zero.small.file bs=1024 count=102400```

- ```dd if=/dev/zero of=zero.file bs=1024```
- ```sync ; sleep 60 ; sync```
- ```rm zero.small.file```
- ```rm zero.file```

Keep in mind all these options need to be applied on the entire physical drive and not on a specific partition/volume. If you do not, wear-leveling mechanisms might prevent this from working properly.

Internal/External HDD drive or a Thumb Drive:

Use the same method as Linux from a Qubes connected to that specific USB device

- You can do this the graphical way with BleachBit following this tutorial from the EFF: https://ssd.eff.org/en/module/how-delete-your-data-securely-linux [Archive.org]
- Or you can do this from the command line following this tutorial: https://linuxhint.com/completely_wipe_hard_drive_ubuntu/ [Archive.org] (For this purpose I recommend wipe and shred).

External SSD drive:

First please see Appendix K: Considerations for using external SSD drives

If Trim is supported and enabled by your Linux Distribution for your external SSD drive. There should be no issue in securely deleting data normally and just issue an "fstrim --all" from terminal to trim the drive. Refer to this Documentation (https://github.com/Qubes-Community/Contents/blob/master/docs/configuration/disk-trim.md [Archive org]) to enable trim on a drive.

If Trim is not supported or you want to be sure, you might have to ensure secure data deletion by filling up the entire free space of the disk using a utility from a Qubes connected to the USB device in question:

- Decrypt and re-encrypt (using LUKS using this tutorial https://wiki.archlinux.org/index.php/dm-crypt/Device_encryption#Re-encrypting_devices [Archive.org] or Veracrypt from the graphical interface for instance) the whole drive to overwrite all free space after data deletion. This will ensure overwriting of all the free space.
- Fill the free space using one of those methods:
  - BleachBit https://www.bleachbit.org/download/linux [Archive.org]
  - Install secure-delete package and use sfill on the root of the drive:
    - ```sudo sfill -l -l /``` for instance should do the trick (this will take a substantial amount of time)
  - Use the old school dd method (taken from this answer https://superuser.com/questions/19326/how-to-wipe-free-disk-space-in-linux [Archive.org]) run these commands:
    - ```dd if=/dev/zero of=zero.small.file bs=1024 count=102400```
    - ```dd if=/dev/zero of=zero.file bs=1024```

Repeat these steps on any other partition if there are separate partitions on the same SSD drive before deleting the files.

- ```sync ; sleep 60 ; sync```
- ```rm zero.small.file```
- ```rm zero.file```

Repeat these steps on any other partition if there are separate partitions on the same SSD drive.

Keep in mind all these options need to be applied on the entire physical drive and not on a specific partition/volume. If you do not, wear-leveling mechanisms might prevent this from working properly.

MacOS:

System/Internal SSD drive:

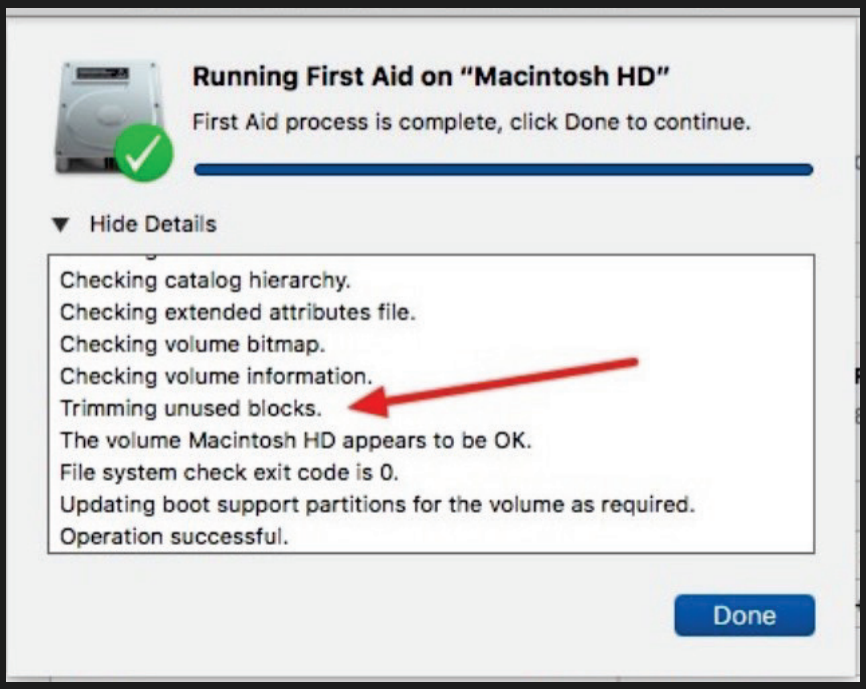
Just permanently delete the file (and empty recycle bin) and it should be unrecoverable due to trim operations and garbage collection.

- If your file system is APFS, you do not need to worry about Trim, it apparently happens asynchronously as the OS writes data[405] according to their own documentation.

"Does Apple File System support TRIM operations?

Yes. TRIM operations are issued asynchronously from when files are deleted or free space is reclaimed, which ensures that these operations are performed only after metadata changes are persisted to stable storage".

- If your file system is HFS+, you could run First Aid on your System Drive from the Disk Utility which should perform a Trim operation in the details (https://support.apple.com/en-us/HT210898 [Archive.org])



System/Internal, External HDD drive or a Thumb Drive:

Unfortunately, Apple has removed the secure erase options from the trash bin even for HDD drives[406]. So, you are left with using other tools:

- Permanent Eraser http://www.edenwaith.com/products/permanent%20eraser/ [Archive.org]
- From the terminal you can use the "rm –P filename" command which should erase the file and overwrite it as explained in this EFF tutorial https://ssd.eff.org/en/module/how-delete-your-data-securely-macos [Archive org].

In the case of USB thumb drives, consider wiping them completely using Disk Utility as instructed previously.

External SSD drive:

First please see Appendix K: Considerations for using external SSD drives

If Trim is supported and enabled by MacOS for your external SSD drive. There should be no issue in securely deleting data.

---

[405] Apple Developer Documentation, https://developer.apple.com/library/archive/documentation/FileManagement/Conceptual/APFS_Guide/FAQ/FAQ.html [Archive org]

[406] EFF, How to: Delete Your Data Securely on MacOS https://ssd.eff.org/en/module/how-delete-your-data-securely-macos [Archive org]

If Trim is not supported, you might have to ensure secure data deletion by:

- Filling up all the free space after any deletion using the Linux Method above (dd).
- Decrypt and Re-encrypt the disk with a different key after each deletion (using Disk Utility or Veracrypt).

Some additional measures against forensics:

Note that the same SSD issue discussed in the previous section will arise here. You can never really be absolutely 100% sure your SSD data is deleted when you ask it to do so unless you wipe the whole drive using specific methods above.

I am not aware of any 100% reliable method to delete single files selectively and securely on SSD drives unless overwriting ALL the free space (which might reduce the lifespan of your SSD) after Deletion + Trim of these files. Without doing that, you will have to trust the SSD Trim operation **which in my opinion is enough**. **It is reasonable and again very unlikely that forensics will be able to restore your files after a Deletion with Trim.**

In addition, most of these measures here should not be needed since your whole drive should be encrypted and therefore your data should not be accessible for forensic analysis through SSD/HDD examination anyway. So, these are just "bonus measures" for weak/unskilled adversaries.

Consider also reading this documentation if you're going with Whonix https://www.whonix.org/wiki/Anti-Forensics_Precautions [Archive.org] as well as their general hardening tutorial for all platforms here https://www.whonix.org/wiki/System_Hardening_Checklist [Archive.org]

Removing Metadata from Files/Documents/Pictures:

Pictures and videos:

On Windows, MacOS and Linux I would recommend ExifTool (https://exiftool.org/ [Archive.org]) and/or ExifCleaner (https://exifcleaner.com/ [Archive.org]) that allows viewing and/or removing those properties.

ExifTool is natively available on Tails and Whonix Workstation.

ExifCleaner:

Just install it from https://exifcleaner.com/ [Archive.org], run and drag and drop the files into the GUI.

ExifTool:

It is actually simple, jut install exiftool and run:

- To display metadata: ```exiftool filename.jpg```
- To remove all metadata: ```exiftool -All= filename.jpg```

Remember that ExifTool is natively available on Tails and Whonix Workstation.

Windows Native tool:

Here is a tutorial to remove metadata from a Picture using OS provided tools: https://www.purevpn.com/internet-privacy/how-to-remove-metadata-from-photos [Archive org]

Cloaking/Obfuscating to prevent picture recognition:

Consider the use of Fawkes https://sandlab.cs.uchicago.edu/fawkes/ [Archive org] (https://github.com/Shawn-Shan/fawkes [Archive.org]) to cloak the images from picture recognition tech on various platforms.

Or if you want on-line versions, consider:

- https://lowkey.umiacs.umd.edu/ [Archive org]
- https://adversarial.io/ [Archive.org]

PDF Documents:

PDFParanoia (Linux/Windows/MacOS/QubesOS):

Consider using https://github.com/kanzure/pdfparanoia [Archive.org] which will remove metadata and watermarks on any PDF.

ExifCleaner (Linux/Windows/MacOS/QubesOS):

Just install it from https://exifcleaner.com/ [Archive.org], run and drag and drop the files into the GUI.

ExifTool (Linux/Windows/MacOS/QubesOS):

It is actually simple, jut install exiftool and run:

- To display metadata: ```exiftool filename.pdf```
- To remove all metadata: ```exiftool -All= filename.pdf```

MS Office Documents:

First, here is a tutorial to remove metadata from Office documents: https://support.microsoft.com/en-us/office/remove-hidden-data-and-personal-information-by-inspecting-documents-presentations-or-workbooks-356b7b5d-77af-44fe-a07f-9aa4d085966f [Archive org]. Make sure however that you do use the latest version of Office with the latest security updates.

Alternatively, on Windows, MacOS, Qubes OS, and Linux I would recommend ExifTool (https://exiftool.org/ [Archive org]) and/or ExifCleaner (https://exifcleaner.com/ [Archive.org]) that allows viewing and/or removing those properties

ExifCleaner:

Just install it from https://exifcleaner.com/ [Archive.org], run and drag and drop the files into the GUI.

ExifTool:

It is actually simple, jut install exiftool and run:

- To display metadata: ```exiftool filename.docx```
- To remove all metadata: ```exiftool -All= filename.docx```

LibreOffice Documents:

Go to Tools > Options > Security and Check:

- All the warnings
- Remove Personal information on saving

Alternatively, on Windows, MacOS, Qubes OS, and Linux I would recommend ExifTool (https://exiftool.org/ [Archive org]) and/or ExifCleaner (https://exifcleaner.com/ [Archive.org]) that allows viewing and/or removing those properties

ExifCleaner:

Just install it from https://exifcleaner.com/ [Archive.org], run and drag and drop the files into the GUI.

ExifTool:

It is actually simple, jut install exiftool and run:

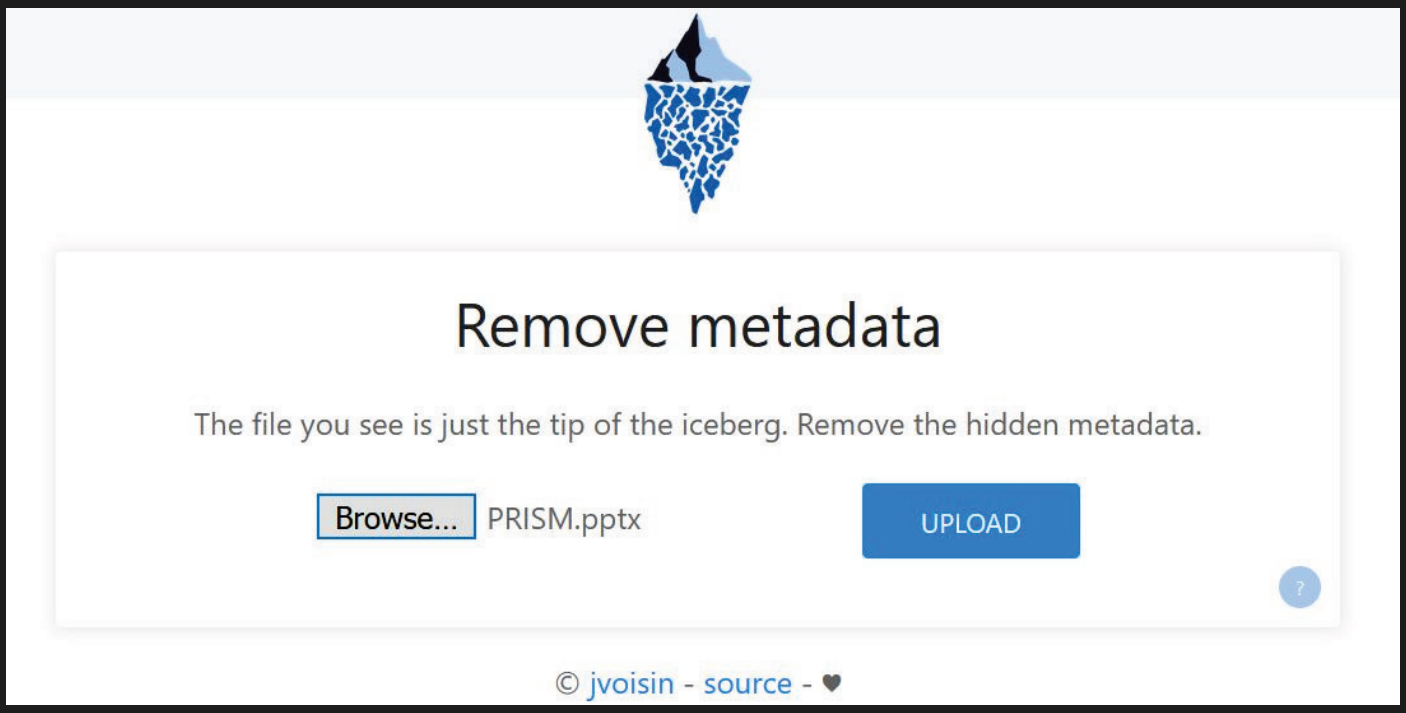
- To display metadata: ```exiftool filename.odt```
- To remove all metadata: ```exiftool -All= filename.odt```

All-in-one Tool:

Another option good tool IMHO to remove metadata from various documents is the open-source mat2 recommended by privacytools.io[407] (https://0xacab.org/jvoisin/mat2 [Archive.org]) which you can use on Linux quite easily. I never managed to make it work properly within Windows due various dependencies issues despite the provided instructions. It is however very straightforward to install and use on Linux.

So, I would suggest creating a small Debian VM within Virtualbox (behind your Whonix Gateway) which you can then use from your other VMs to analyze various files from a convenient web interface. For this see Appendix L: Creating a mat2-web guest VM for removing metadata from files

[407] Privacytools.io, Productivity tools https://www.privacytools.io/software/productivity/ [Archive.org]



Mat2 is also pre-installed on the Whonix Workstation VM[408] and available on Tails by default[409].

Tails:

Tails is great for this; you have nothing to worry about even if you use an SSD drive. Shut it down and it is all gone as soon as the memory decays.

Whonix:

Note that it's possible to run Whonix in Live mode leaving no traces when you shut down the VMs, consider reading their documentation here https://www.whonix.org/wiki/VM_Live_Mode [Archive.org] and here https://www.whonix.org/wiki/Warning#Whonix_.E2.84.A2_Persistence_vs_Live_vs_Amnesic [Archive.org].

MacOS:

Guest OS:

Revert to a previous snapshot on Virtualbox (or any other VM software you are using) and perform a Trim command on your Mac using Disk Utility by executing a first-aid on the Host OS again as explained at the end of the next section.

Host OS:

Most of the info from this section can also be found at this nice guide https://github.com/drduh/macOS-Security-and-Privacy-Guide [Archive.org]

Quarantine Database (used by Gatekeeper and XProtect):

MacOS (up to and included Big Sur) keeps a Quarantine SQL Database of all the files you ever downloaded from a Browser. This database is located at ```~/Library/Preferences/com.apple.LaunchServices.QuarantineEventsV2```.

You can query it yourself by running the following command from terminal: ``` sqlite3 ~/Library/Preferences/com.apple.LaunchServices.QuarantineEventsV2 "select * from LSQuarantineEvent" ```

Obviously, this is a goldmine for forensics and you should disable this:

- Run the following command to clear the database completely: ```:>~/Library/Preferences/com.apple.LaunchServices.QuarantineEventsV2```

[408] Whonix Documentation, Scrubbing Metadata https://www.whonix.org/wiki/Metadata [Archive.org]

[409] Tails documentation, MAT https://gitlab.tails.boum.org/tails/blueprints/-/wikis/doc/mat/ [Archive.org]

- Run the following command to lock the file and prevent further download history from being written there: ```sudo chflags schg ~/Library/Preferences/com.apple.LaunchServices.QuarantineEventsV2```

Lastly you can also disable Gatekeeper altogether by issuing the following command in terminal[410]:

- ```sudo spctl --master-disable```

Refer to this section of this guide for further information https://github.com/drduh/macOS-Security-and-Privacy-Guide#gatekeeper-and-xprotect [Archive.org]

In addition to this convenient database, each saved file will also carry detailed file system HFS+/APFS attributes showing for instance when it was downloaded, with what and from where.

You can view these just by opening a terminal and typing ```mdls filename``` and ```xattr -l filename``` on any downloaded file from any browser.

To remove such attributes, you will have to do it manually from the terminal:

- Run ```xattr -d com.apple.metadata:kMDItemWhereFroms filename``` to remove the origin
  - You can also just use -dr to do it recursively on a whole folder/disk
- Run ```xattr -d com.apple.quarantine filename``` to remove the quarantine reference
  - You can also just use -dr to do it recursively on a whole folder/disk
- Verify by running ```xattr –l filename``` and there should be no output

(Note that Apple has removed the convenient xattr –c option that would just remove all attributes at once so you will have to do this for each attribute on each file)

These attributes and entries will stick even if you clear your Browser history and this is obviously bad for privacy (right?) and I am not aware of any convenient tool that will deal with those at the moment.

Fortunately, there are some mitigations for avoiding this issue in the first place as these attributes and entries are set by the browsers. So, I tested various browsers (On MacOS Catalina and Big Sur) and here are the results as of the date of this guide:

Browser	Quarantine DB Entry	Quarantine File Attribute	Origin File Attribute
Safari (Normal)	Yes	Yes	Yes
Safari (Private Window)	No	No	No
Firefox (Normal)	Yes	Yes	Yes
Firefox (Private Window)	No	No	No
Chrome (Normal)	Yes	Yes	Yes
Chrome (Private Window)	Partial (timestamp only)	No	No
Ungoogled-Chromium (Normal)	No	No	No
Ungoogled-Chromium (Private Window)	No	No	No
Brave (Normal)	Partial (timestamp only)	No	No
Brave (Private Window)	Partial (timestamp only)	No	No
Brave (Tor Window)	Partial (timestamp only)	No	No
Tor Browser	No	No	No

As you can see for yourself the easiest mitigation is to just use Private Windows. These do not write those origin/quarantine attributes and do not store the entries in the QuarantineEventsV2 database.

Clearing the QuarantineEventsV2 is easy as explained above. Removing the attributes takes some work. **Brave is the only tested browser that will not store those attributes by default in normal operations.**

[410] GitHub, Disable Gatekeeper on macOS Big Sur (11.x) https://disable-gatekeeper.github.io/ [Archive.org]

Various Artifacts:

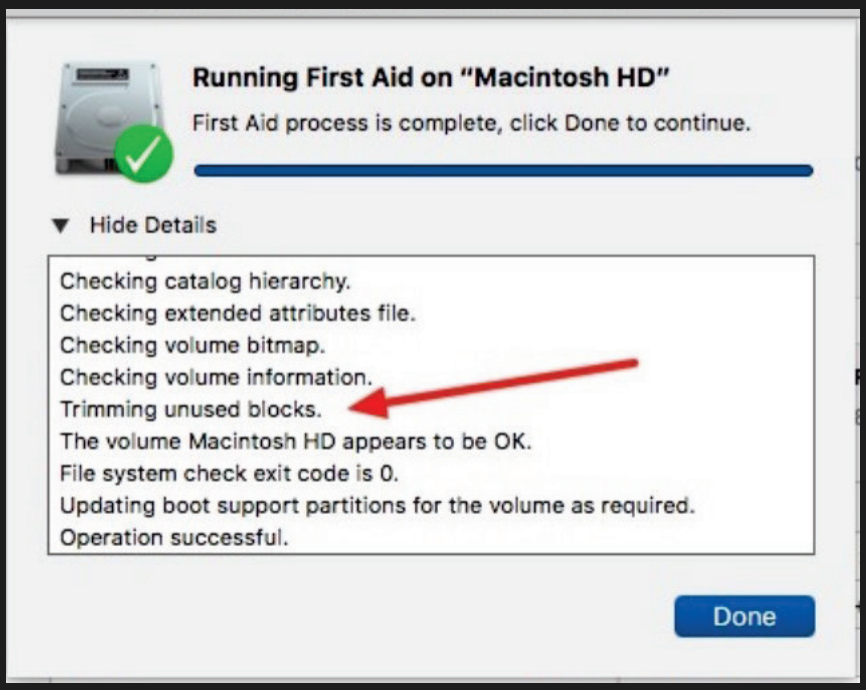
In addition, MacOS keeps various logs of mounted devices, connected devices, known networks, analytics, documents revisions…

See this section of this guide for guidance on where to find and how to delete such artifacts: https://github.com/drduh/macOS-Security-and-Privacy-Guide#metadata-and-artifacts [Archive.org]

Many of those can be deleted using some various commercial third-party tools but I would personally recommend using the free and well-known Onyx which you can find here: https://www.titanium-software.fr/en/onyx.html [Archive org]. Unfortunately, it is closed-source but it is notarized, signed and has been trusted for many years.

Force a Trim operation after cleaning:

- If your file system is APFS, you do not need to worry about Trim, it happens asynchronously as the OS writes data.
- If your file system is HFS+ (or any other than APFS), you could run First Aid on your System Drive from the Disk Utility which should perform a Trim operation in the details (https://support.apple.com/en-us/HT210898 [Archive.org]).



Linux (Qubes OS):

Please consider their guidelines https://github.com/Qubes-Community/Contents/blob/master/docs/security/security-guidelines.md [Archive.org]

If you are using Whonix on Qubes OS, please consider following some of their guides:

- Whonix System Hardening guide https://www.whonix.org/wiki/System_Hardening_Checklist [Archive.org]
- Enabling App Armor on Qubes https://www.whonix.org/wiki/Qubes/AppArmor [Archive org]
- Also consider the use of Linux Kernel Guard https://www.whonix.org/wiki/Linux_Kernel_Runtime_Guard_LKRG [Archive.org]

Linux (non-Qubes):

Guest OS:

Revert to a previous snapshot of the Guest VM on Virtualbox (or any other VM software you are using) and perform a trim command on your laptop using ```fstrim --all```. This utility is part of the ```util-linux``` package on Debian/Ubuntu and should be installed by default on Fedora. Then switch to the next section.

Host OS:

Normally you should not have traces to clean within the Host OS since you are doing everything from a VM if you follow this guide.

Nevertheless, you might want to clean some logs. Just use this convenient tool: https://github.com/sundowndev/go-covermyass [Archive.org] (instructions on the page)

After cleaning up, make sure you have the fstrim utility installed (should be by default on Fedora) and part of the ```util-linux``` package on Debian/Ubuntu. Then just run ```fstrim --all``` on the Host OS. This should be sufficient on SSD drives as explained earlier.

Consider the use of Linux Kernel Guard as an added measure
https://www.whonix.org/wiki/Linux_Kernel_Runtime_Guard_LKRG [Archive.org]

Windows:

Guest OS:

Revert to a previous snapshot on Virtualbox (or any other VM software you are using) and perform a trim command on your Windows using the Optimize as explained in the end of the next section

Host OS:

Now that you had a bunch of activities with your VMs or Host OS, you should take a moment to cover your tracks. **Most of these steps should not be undertaken on the Decoy OS in case of use of plausible deniability. This is because you want to keep decoy/plausible traces of sensible but not secret activities available for your adversary. If everything is clean then you might raise suspicion.**

Diagnostic Data and Telemetry:

First let us get rid of any diagnostic data that could still be there:

(Skip this step if you are using Windows 10 AME)

- After each use of your Windows devices, go into Settings, Privacy, Diagnostic & Feedback, and Click Delete.

Then let us re-randomize the MAC addresses of your Virtual Machines and the Bluetooth Address of your Host OS.

- After each shutdown of your Windows VM, change its MAC address for next time by going into Virtualbox > Select the VM > Settings > Network > Advanced > Refresh the MAC address.
- After each use of your Host OS Windows (your VM should not have Bluetooth at all), Go into the Device Manager, Select Bluetooth, Disable Device and Re-Enable device (this will force a randomization of the Bluetooth Address).

Event logs:

Windows Event logs will keep many various pieces of information that could contain traces of your activities such as the devices that were mounted (including Veracrypt NTFS volumes for instance[294]), your network connections, app crash information and various errors. It is always best to clean those up regularly. Do not do this on the Decoy OS.

- Start, search for Event Viewer, and launch Event Viewer:
  - Go into Windows logs.
  - Select and clear all 5 logs using right click.

Veracrypt History:

By default, Veracrypt saves a history of recently mounted volumes and files. You should make sure Veracrypt never saves History. Again, do not do this on the Decoy OS if you are using plausible deniability for the OS. We need to keep the history of mounting the decoy Volume as part of the plausible deniability.

- Launch Veracrypt
- Make sure the "Never saves history" checkbox is checked (this should not be checked on the Decoy OS)

Now you should clean the history within any app that you used including Browser history, Cookies, Saved Passwords, Sessions, and Form History.

Browser History:

- Brave (in case you did not enable cleaning on exit)
  - Go into Settings

    - Go into Shields
    - Go into Clear Browsing Data
    - Select Advanced
    - Select "All Time"
    - Check all the options
    - Clear Data
- Tor Browser
    - Just close the Browser and everything is cleaned

Wi-Fi History:

Now it is time to clear the history of the Wi-Fi you connect to. Unfortunately, Windows keeps storing a list of past Networks in the registry even if you "forgot" those in the Wi-Fi settings. As far as I know, no utilities clean those yet (BleachBit or PrivaZer for instance) so you will have to do it the manual way:

- Launch Regedit using this tutorial: https://support.microsoft.com/en-us/windows/how-to-open-registry-editor-in-windows-10-deab38e6-91d6-e0aa-4b7c-8878d9e07b11 [Archive.org]
- Within Regedit, enter this to the address bar:
  ```Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles```
- There you will see a bunch of folders to the right. Each of those folders is a "Key". Each of those keys will contain information about your current known Wi-Fi or past networks you used. You can explore them one by one and see the description on the right side.
- Delete all those keys.

Shellbags:

As explained earlier, Shellbags are basically histories of accessed volumes/files on your computer. Remember that shellbags are very good sources of information for forensics[287] and you need to clean those. Especially if you mounted any "hidden volume" anywhere. Again, you should not do this on the Decoy OS.

    - Download Shellbag Analyzer & Cleaner from https://privazer.com/en/download-shellbag-analyzer-shellbag-cleaner.php [Archive.org]
        - Launch it
        - Analyze
        - Click Clean and select:
            - Deleted Folders
            - Folders on Network / External devices
            - Search Results
        - Select advanced
            - Check all except the two backup options (do not backup)
            - Select SSD cleanup (if you have an SSD)
            - Select 1 pass (All zero)
            - Clean

Extra Tools Cleaning:

After cleaning those previous traces, you should also use third party utilities than can be used to clean various traces. These include the traces of the files/folders you deleted.

Please refer to Appendix H: Windows Cleaning Tools before continuing.

PrivaZer:

Here are the steps for PrivaZer:

- Download and install PrivaZer from https://privazer.com/en/download.php [Archive.org]
    - Run PrivaZer after install
    - Do not use their Wizard
    - Select Advanced User
  ```

- Select Scan in Depth and pick your Target
- Select Everything you want to Scan and push Scan
- Select What you want cleaned (skip the shell bag part since you used the other utility for that)
  - **You should just skip the free space cleaning part if using an SSD and instead just use the native Windows Optimize function (see below) which should be more than enough. I would only use this on an HDD drive.**
- (If you did select Free Space cleaning) Select Clean Options and make sure your type of Storage if well detected (HDD vs SSD).
- (If you did select Free Space cleaning) Within Clean Options **(Be careful with this option as it will erase all the free space on the selected partition, especially if you are running the decoy OS. Do not erase the free space or anything else on the second partition as you risk destroying your Hidden OS)**
  - If you have an SSD drive:
    - Secure Overwriting Tab: Personally, I would just pick Normal Deletion + Trim (Trim itself should be enough[298]). Secure Deletion with Trim[295] (1 pass) might be redundant and overkill here if you intend to overwrite the free space anyway.
    - Free Space Tab: Personally, and again "just to be sure", I would select Normal Cleanup which will fill the entire free space with Data. I do not really trust Smart Cleanup as it does not actually fill all the free space of the SSD with Data. But again, I think this is probably not needed and overkill in most cases.
  - If you have an HDD drive:
    - Secure Overwriting Tab: I would just pick Secure Deletion (1 pass).
    - Free Space: I would just pick Smart Cleanup as there is no reason to overwrite sectors without data on an HDD drive.
- Select Clean and Pick your flavor:
  - Turbo Cleanup will only do normal deletion (on HDD/SSD) and will not clean free space. It is not secure on an HDD nor an SSD.
  - Quick Cleanup will do secure deletion (on HDD) and normal deletion + trim (on SSD) but will not clean free space. I think this is secure enough for SSD but not for HDD.
  - Normal Cleanup will do secure deletion (on HDD) and normal deletion + trim (on SSD) and will then clean the whole free space (Smart Cleanup on HDD and Full Cleanup on SSD) and should be secure. I think this option is the best for HDD but completely overkill for SSD.
- Click Clean and wait for cleaning to finish. Could take a while and will fill your whole free space with data.

BleachBit:

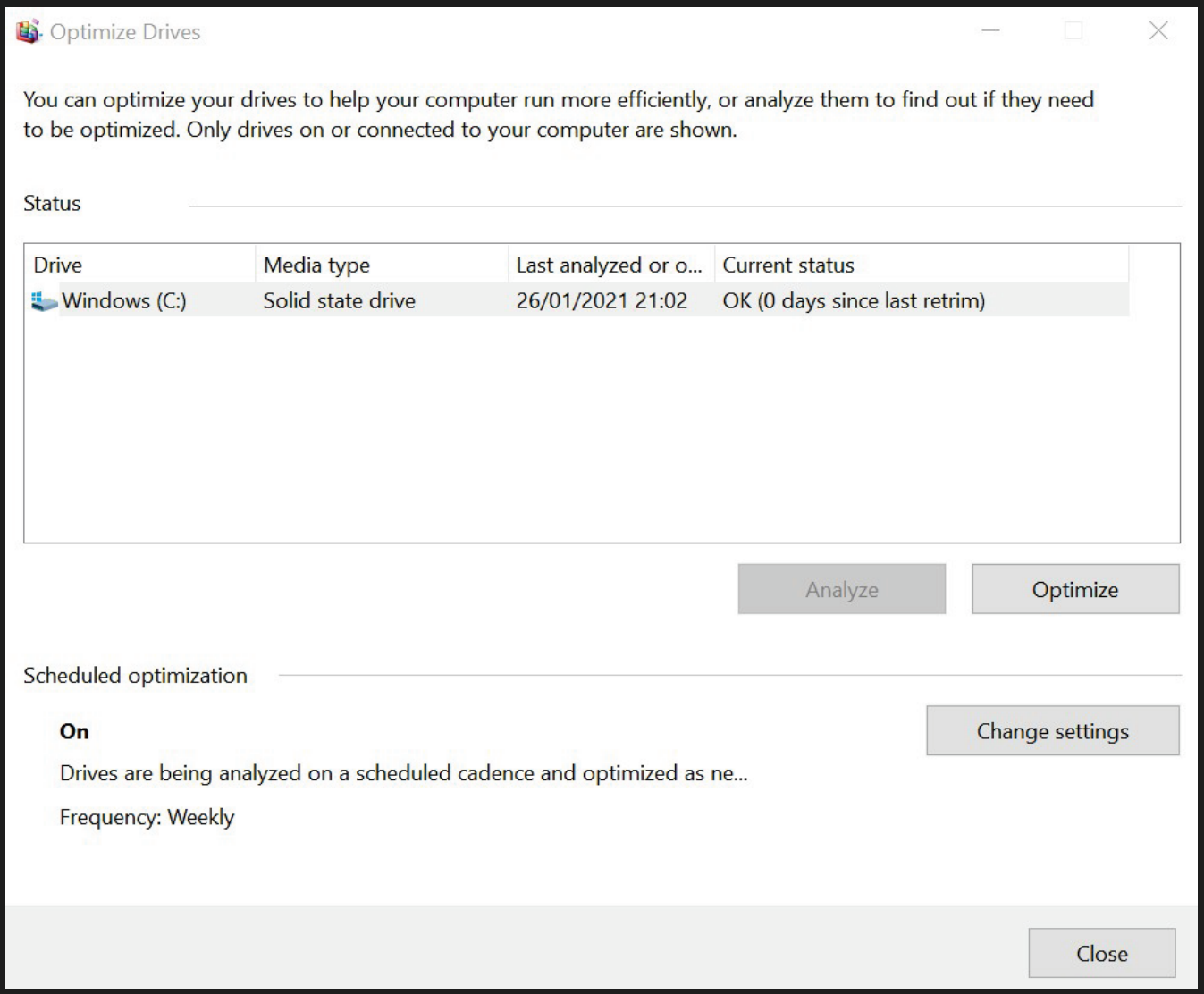
Here are the steps for BleachBit:

- Get and install the latest version from BleachBit here https://www.bleachbit.org/download [Archive org]
- Run BleachBit
- Clean at least everything within those sections:
  - Deep Scan
  - Windows Defender
  - Windows Explorer (including Shellbags)
  - System
  - Select any other traces you want to remove from their list
    - Again, as with the previous utility, I would not clean the free space on an SSD drive because I think the Windows native "optimize" utility is enough (see Below) and that filling up the free space on a trim enabled SSD is just completely overkill and unnecessary.
  - Click Clean and wait. This will take a while and will fill your whole free space with data on both HDD and SSD drives.

Force a Trim with Windows Optimize (for SSD drives):

With this Native Windows 10 utility, you can just trigger a Trim on your SSD which should be more than enough to securely clean all deleted files that somehow would have escaped Trim when deleting them.

Just open Windows Explorer, Right Click on your System Drive and click Properties. Select Tools. Click Optimize and then Optimize again. You are done. I think that is probably enough in my opinion.



Removing some traces of your identities on search engines and various platforms:

Chances are your actions (such as posts on various platforms, your profiles) will be indexed (and cached) by many search engines.

Contrary to popular belief, it is possible to have some but not all this information removed by following some steps. While this might not remove the information on the websites themselves, it will make it harder for people to find it using search engines.

- First, you will have to delete your identities from the platform themselves if you can. Most will allow this but not all. For some you might have to contact their support/moderators and for others there will be readily available forms to do so.
- If they do not allow removal/deletion of profiles, there might be a possibility for you to rename your identity. Change the username if you can and all account information with bogus information including the e-mail.
- If allowed, you can also sometimes edit past posts to remove the information within those.

You can check some useful information about how to and get delete various accounts on these websites:

- https://justdeleteme.xyz/ [Archive.org]

- https://justgetmydata.com/ [Archive.org]

When you are done with this part, you should now handle search engines and while you may not be able to have the information deleted, you can ask them to update/remove outdated information which could then remove some cached information.

Google:

Unfortunately, this will require you to have a Google account to request the update/removal (however this can be done with any Google account from anyone). There is no way around this except waiting.

Go to their "Remove outdated content from Google Search" page here: https://search.google.com/search-console/remove-outdated-content [Archive.org] and submit a request accordingly.

If your profile/username was deleted/changed, they should re-index the content and update accordingly and remove these traces.

These requests might take several days to process. Be patient.

Bing:

Unfortunately, this will require you to have a Microsoft account to request the update/removal (however this can be done with any Microsoft account from any identity). There is no way around this except waiting.

Go to their "Content Removal" page here: https://www.bing.com/webmasters/tools/contentremoval [Archive.org] and submit a request accordingly.

If your profile/username was deleted/changed, they should re-index the content and update accordingly and remove these traces.

This might take several days to process. Be patient.

DuckDuckGo:

DuckDuckGo does not store cached version of pages[411] and will instead forward you to a Google/Bing cached version if available.

In addition, DuckDuckGo source most of their searches from Bing (and not google)[412] and therefore removing the content from Bing should in time have it removed it from DuckDuckGo too.

Yandex:

Unfortunately, this will require you to have a Yandex account to request removals (however this can be done with any Yandex account from any identity). There is no way around this except waiting.

Once have your Yandex account, head to the Yandex Webmaster tools https://webmaster.yandex.com [Archive.org] and then select Tools and Delete URL https://webmaster.yandex.com/tools/del-url/ [Archive.org]

There you can input the URL that do not exist anymore if you had them deleted.

This will only work with pages that have been deleted and therefore will not work with removing cache of existing records. For that unfortunately there is no tool available to force a cache update but you can still try their feedback tool:

Search for the page that was changed (where your profile was deleted/changed) and click the arrow next to the result. Select Complain. And submit a complaint about the page not matching the search result. Hopefully this will force Yandex to re-crawl the page and re-index it after some time. This could take days or weeks.

---

[411] DuckDuckGo help, Cache https://help.duckduckgo.com/duckduckgo-help-pages/features/cache/ [Archive.org]

[412] DuckDuckGo help, Sources https://help.duckduckgo.com/duckduckgo-help-pages/results/sources/ [Archive.org]

Qwant:

As far as I know, there is no readily available tool to force this and you will have to wait for the results to get updated if there is any. If you know a way, please report this to me through the GitHub issues.

Yahoo Search:

Yes, Yahoo Search still exists but as per their help page https://help.yahoo.com/kb/SLN4530.html [Archive.org] , there is no way to remove information or refresh information besides waiting. This could take 6 to 8 weeks.

Baidu:

As far as I know, there is no readily available tool to force this unless you control the website (and do it through their webmaster tools). Therefore, you will have to wait for the results to get updated if there is any. If you know a way, please report this to me through the GitHub issues.

Wikipedia:

As far as I know, there is no way to remove information from Wikipedia articles themselves but if you just want to remove traces of your username from it (as a user that contributed), you can do so by following these steps: https://en.wikipedia.org/wiki/Wikipedia:Courtesy_vanishing [Wikiless] [Archive.org]

This will not remove any information about your online identities that could appear in other articles but only your own identity on Wikipedia as a user.

Archive.today:

Some information can sometimes be removed on demand (sensitive information for example) as you can see many examples here: https://blog.archive.today/archive

This is done through their "ask" page here: https://blog.archive.today/ask

Internet Archive:

You can remove pages from internet archives but **only if you own the website in question** and contact them about it. Most likely you will not be able to remove archives from say "Reddit posts" or anything alike. But you could still ask and see what they answer.

As per their help page https://help.archive.org/hc/en-us/articles/360004651732-Using-The-Wayback-Machine

"How can I exclude or remove my site's pages from the Wayback Machine?

You can send an e-mail request for us to review to info@archive.org with the URL (web address) in the text of your message".

Some low-tech old-school tricks:

Hidden communications in plain sight:

You must keep in mind that using all those security measures (encryption, plausible deniability, VPN, tor, secure operating systems …) can make you suspicious just by using them. Using could be the equivalent of stating openly "I have something to hide" to an observer which could then motivate some adversaries to investigate/survey you further.

So, there are other ways you could exchange or send messages online to others in case of need without disclosing your identity or establishing direct communication with them. These have been in use by various organizations for decades and can be of help if you do not want to attract attention by using secure tech while still communicating some sensitive information without attracting attention.

A commonly used technique which combines the idea of a Dead Drop[413] and Secure Communication Obfuscation[414] through Steganography[415] and/or Kleptography[416] and has many names such as Koalang[417] or "Talking Around" or even "Social Steganography". This technique is very old and still widely used nowadays by teenagers to bypass parental control. It is hiding in plain sight.

Here is one example if you want to let someone know something is wrong and they should go dark? That they should immediately wipe all their data, get rid of their burner phones and sensitive information?

What if you want to let someone you trust (friends, family, lawyers, journalists …) know that you are in trouble and they should look out for you?

All this without revealing the identity of the person you are sending the message to nor disclosing the content of that message to any third party and without raising suspicions and without using any of the secure methods mentioned above.

Well, you could just use any online public platform for this (Instagram, Twitter, Reddit, any forum, YouTube …) by using in-context (of the chosen platform/media) agreed upon (between you and your contact) coded messages that only your contact would understand.

This could be a set of specific Emoji's or a specifically worded mundane comment. Or even just a like on a specific post from a known influencer you usually watch and like. While this would look completely normal to anyone, this could in fact mean a lot to a knowledgeable reader who could then take appropriate agreed upon actions. You could also hide the message using Steganography using for instance https://stegcloak.surge.sh/.

You do not even have to go that far. A simple "Last seen" time on a specific account could be enough to trigger a message agreed upon. If your interlocutor sees that such account was online. It could mean there is an issue.

How to spot if someone has been searching your stuff:

There are some old tricks that you can use to spot if people have been messing with your stuff while you were away.

One trick for instance is very simple and just requires a wire/cable. Simply dispose objects on your desk/night table or in your drawers following a straight line. You can use a simple USB cable as a tool to align them.

Make a line with your cable and place objects along the line. When you are back, just check those places and check if the objects are still placed along the line. This allows you not to remember precisely where your things were without taking pictures.

Fortunately, modern technology has made this even simpler. If you suspect someone might be looking through your stuff while you are away, you can just take a picture of the area with your phone before leaving. When you are back, just compare the areas with your pictures and everything should be exactly where you left it. If anything moved then someone was there.

It will be very hard and time consuming for an adversary to search through your stuff and then replace it exactly as you left it with complete precision.

What if it is a printed document or book and you want to know if someone read it? Even simpler. Just carefully make a note within the document with a pencil. And then erase it with any pencil eraser as if you wanted to correct it. The trick is to carefully leave the eraser traces/residues on the area you erased/pencil written areas and close the document. You could also take a picture of the residues before closing the document.

---

[413] Wikipedia, Dead Drop https://en.wikipedia.org/wiki/Dead_drop [Wikiless] [Archive.org]

[414] Wikipedia, Secure Communication Obfuscation https://en.wikipedia.org/wiki/Obfuscation#Secure_communication [Wikiless] [Archive org]

[415] Wikipedia, Steganography https://en.wikipedia.org/wiki/Steganography [Wikiless] [Archive.org]

[416] Wikipedia, Kleptography https://en.wikipedia.org/wiki/Kleptography [Wikiless] [Archive.org]

[417] Wikipedia, Koalang https://en.wikipedia.org/wiki/Koalang [Wikiless] [Archive.org]

Most likely if someone went through your document to read it and re-placed it carefully, this residue will fall off or be moved significantly. It is a simple old school trick that could tell you someone searched a document you had.

Some last OPSEC thoughts:

Wait, what is OPSEC? Well, OPSEC means Operations Security[418]. The basic definition is: "OPSEC is the process of protecting individual pieces of data that could be grouped together to give the bigger picture ".

OPSEC is often just applying common sense and being cautious about your activities including in the physical world.

- **Remember to use passphrases instead of passwords and use a different one for each service (Appendix A2: Guidelines for passwords and passphrases).**
- Make sure you are not keeping a copy of this guide anywhere unsafe after. The sole presence of this guide will most likely defeat all your plausible deniability possibilities.
- Consider the use of Haven https://guardianproject.github.io/haven/ [Archive.org] on some old android phone to keep watch on your home/room while you are away.
- Doxx "yourself" and your identities from time to time by looking for them yourself online using various search engines to monitor your online identities. You can even automate the process somewhat using various tools such as Google Alerts https://www.google.com/alerts [Archive.org].
- Remember Appendix N: Warning about smartphones and smart devices. Do not forget your smart devices can compromise your anonymity.
- Do not ever use biometrics alone to safeguard your secrets. Biometrics can be used without your consent.
- Do not ever travel with those devices if you must pass strong border checks and where they could be illegal or raise suspicion.
- Do not plug any equipment in that laptop unless you trust it. Use an USB data blocker for charging.
- Do check the signatures and hashes of Software you download before installing them.
- Remember the first rule of fight club and do not talk to anyone about your sensitive activities using your real identity.
- Keep a normal life and do not be weird. If you spend all your online time using Tor to access the internet and have no social network accounts at all … You are already suspicious and attracting unnecessary attention.
- Encrypt everything but do not take it as granted. Remember the 5$ wrench[11] .
- Keep plausible deniability as an option but remember it will not help against the 5$ wrench either[11].
- Never ever leave your laptop unattended/on/unlocked anywhere when conducting sensitive activities. Remember the story of Ross Ulbricht and his arrest https://en.wikipedia.org/wiki/Ross_Ulbricht#Silk_Road,_arrest_and_trial [Wikiless] [Archive.org].
- Check for tampering regularly (not only your devices but also your home/room).
- If you can, do not talk to the police/authorities (at least if you are in the US) https://www.youtube.com/watch?v=d-7o9xYp7eE [Invidious] without a lawyer. Remain silent.
- Know and always have at your disposal the details of a lawyer that could help you as a last resort in case things go wrong.
- Read those tips here https://www.whonix.org/wiki/DoNot [Archive.org]
- **Finally, have common sense, do not be dumb, look and learn from others' mistakes, watch these:**
    - 2020, Sinwindie, OSINT and Dark Web Markets, Why OPSEC Still Matters https://www.youtube.com/watch?v=IqZZU9lFlF4 [Invidious]
    - 2020, RSA Conference 2020, When Cybercriminals with Good OpSec Attack https://www.youtube.com/watch?v=zXmZnU2GdVk [Invidious]
    - 2015, DEFCON 22, Adrian Crenshaw- Dropping Docs on Darknets: How People Got Caught, https://www.youtube.com/watch?v=eQ2OZKitRwc [Invidious] (Slides [Archive.org])
    - 2017, Ochko123 - How the Feds Caught Russian Mega-Carder Roman Seleznev https://www.youtube.com/watch?v=6Chp12sEnWk [Invidious]
    - 2015, DEF CON 22 - Zoz - Don't Fuck It Up! https://www.youtube.com/watch?v=J1q4Ir2J8P8 [Invidious]

[418] Wikipedia, OPSEC https://en.wikipedia.org/wiki/Operations_security [Wikiless] [Archive.org]

- 2020, Bad Opsec - How Tor Users Got Caught, https://www.youtube.com/watch?v=GR_U0G-QGA0 [Invidious]

FINAL OPSEC DISCLAIMER: KEEP YOUR ANONYMOUS IDENTITIES COMPLETELY SANDBOXED FROM YOUR NORMAL ENVIRONMENT AND REAL IDENTITY. DO NOT SHARE ANYTHING BETWEEN THE ANONYMOUS ENVIRONMENTS AND THE REAL IDENTITY ENVIRONMENT. KEEP THEM COMPLETELY COMPARTIMENTALIZED ON EVERY LEVEL. MOST OPSEC FAILURES ARE DUE TO USERS ACCIDENTALY LEAKING INFORMATION RATHER THAN TECHNICAL FAILURES.

If you think you got burned:

If you have some time:

- Don't Panic.
- Delete everything you can from the internet related to that specific identity (accounts, comments …).
- Delete everything offline you have related to that identity including the backups.
- (If using a physical SIM) Destroy the SIM card and trash it in a random trash can somewhere.
- (If using a physical Burner Phone) Erase then destroy the Burner phone and trash it in a random trashcan somewhere.
- Securely erase the laptop hard drive and then ideally proceed to physically destroy the HDD/SSD/Laptop and trash it somewhere.
- Do the same with your backups.
- Keep the details of your lawyer nearby or if needed, call him/her in advance to prepare your case if needed.
- Return to your normal activities and hope for the best.

If you have no time:

- Don't Panic.
- Try to shut down/hibernate the laptop as soon as possible and hope for the best. If you are fast enough, your memory should decay or be cleaned and your data should be mostly safe for the time being.
- Contact a lawyer if possible and hope for the best and if you cannot contact one (yet), **try to remain silent (if your country allows it) until you have a lawyer to help you and if your law allows you to remain silent.**

Keep in mind that many countries have specific laws to compel you to reveal your passwords that could override your "right to remain silent". See this Wikipedia article: https://en.wikipedia.org/wiki/Key_disclosure_law [Wikiless] [Archive org] and this other visual resource with law references https://www.gp-digital.org/world-map-of-encryption/ [Archive org].

A small final editorial note:

After reading this whole guide, I hope you will have gained some additional beneficial insight about privacy and anonymity. It is clear now, in my humble opinion, that the world we live in has only few safe harbors remaining where one could have a reasonable expectation of privacy and even less so anonymity. Many will often say that 1984 by George Orwell was not meant to be an instruction book. Yet today this guide and its many references should, I hope, reveal to you how far down we are in the rabbit hole.

You should also know that most of the digital information described in lengths in this guide can be forged or tampered by a motivated adversary for any purpose. Even if you do manage to keep secrets from prying eyes, it is possible for anyone to fabricate anything to fit their narrative.

- IP logs, DNS logs, Geolocation logs and Connection logs can be forged or tampered with by anyone using a simple text editor without leaving traces.
- Files and their properties can be created, altered, and timestamped by anyone using simple utilities without leaving traces.
- EXIF information of pictures and videos can be altered by anyone using simple utilities without leaving traces.

- Digital Evidence (Pictures, Videos, Voice Recordings, E-Mails, Documents…) be crafted, placed, removed, or destroyed with ease without leaving traces.

You should not hesitate to question this type of information from any source in this age of disinformation.

"A lie can travel half way around the world while the truth is putting on its shoes." -- Mark Twain.

Please keep thinking for yourself and be open to critical thinking. Please keep an open mind. Dare to know!

"In the end the Party would announce that two and two made five, and you would have to believe it." -- George Orwell, 1984.

Donations:

This project has no funding and donations are welcome.

Current Goals:

- **Extend time for**
  - **Tor-Exit-01 node hosting (current expiration date is September 30, 2021. About 60$-54€/year needed total for this.**
  - **Tor-Exit-02 node hosting (current expiration date is December 31, 2021. About 60$-54€/year needed total for this.**
- **Move VPS for the Tor .onion hosting (current expiration date is April 1st, 2022) to a cheaper hosting provider and extend for 2 more years. About 60$-54€/year needed total for this.**
- **Run more Tor Exit nodes if enough funding!**

Donate at https://anonymousplanet.org/donations.html [Mirror] [Archive org] [Tor Mirror] or directly by sending Monero (XMR) to this address:
```4549BGJrEPBfpiPRL9CVGzGMgJnC1Dzf8EXLVfY8Ukrnj7LzkTV611dGf9tuQHiSQjbixsNWiffNiV5fPB3LkyF7UXi3vwQ```

(Please do verify the checksum and gpg signature of this file for authenticity, this is explained in the README of the repository if you do not know how to do that).

Bitcoin (BTC) to these addresses:

- SegWit address: ```bc1qtall24j005qsd3dw8wahxhvged4vepn9fjp3my```
- Legacy address: ```17jYYV1x92fm9EVDbHuQjS5t9Qc44533Jw```

Note that these addresses are being changed at each release but the old ones remain valid.
```

Bitcoin SegWit

Bitcoin Legacy

(Please do verify the checksum and gpg signature of this file for authenticity, this is explained in the README of the repository if you do not know how to do that).

Helping others staying anonymous:

If you want to give a hand to users facing censorship and oppression, please consider helping them by helping the Tor Network. You can do so in several ways:

- The Easiest:
  - Using the Snowflake addon on your browser (https://snowflake.torproject.org/ [Archive.org])
- Slightly more work:
  - Running a Tor relay node (https://community.torproject.org/relay/ [Archive.org])
    - See Recommended VPS hosting providers
    - Additional Tutorial: https://torrelay.ca/ [Archive.org]

If you want a bit more challenge, you can also run a Tor Exit node anonymously using the recommended VPS providers above.

For this, see https://blog.torproject.org/tips-running-exit-node [Archive org]

This project for instance is running a Tor Exit node using the donations from readers. You can see it here: https://metrics.torproject.org/rs.html#details/970814F267BF3DE9DFF2A0F8D4019F80C68AEE26 [Archive.org]

Acknowledgements:

- **Huge thanks to the people who donated to this project anonymously.**
- Thanks to GitHub for hosting this project and the many people who starred it
- Thanks to Njal.la for providing a domain name and hosting anonymously
- Thanks to 1984.is for providing hosting anonymously
- Thanks to all the people who contributed and shared this guide to others
- Thanks to the people at the Internet Archive and Archive.today projects
- Thanks to the people at the Monero project
- Thanks to the people at the Wikipedia project
- Thanks to the people at the Tails project
- Thanks to the people at the HiddenVM project
- Thanks to the people at the Whonix project
- Thanks to the people at the Qubes OS project
- Thanks to the people at the Veracrypt project
- Thanks to the people at the Tor and OONI Projects
- Thanks to the people at the Briar project
- Thanks to the people at the OnionShare project
- Thanks to the people at the Element/Matrix project
- Thanks to the people at the Jami project
- Thanks to the people at the KeePass and KeePassXC projects
- Thanks to the people at the Fawkes project

- Thanks to the people at the VirtualBox project
- Thanks to the people at the ExifCleaner, Mat2 and ExifTool projects
- Thanks to the people at the Go Incognito Project from Techlore
- Thanks to Didier Stevens for his pdf-tools
- Thanks to the people at the EFF
- Thanks to the people at the SANS
- Thanks to the people at the OWASP Project
- Thanks to the people at the Privacytools.io project
- Thanks to the people at BlackHat, DEF CON and CCC
- Thanks to the people at Bellingcat and other OSINT/Forensics researchers **(and sorry for making their life more difficult with this guide)**
- Thanks to the makers of the Social Dilemma documentary **(go watch it if you did not yet)**
- Thanks to Michael Bazzell and his great OSINT books which I recommend you **buy** at https://inteltechniques.com
- Thanks to Randall Munroe at XKCD for his great and insightful webcomics.
- Thanks to NobodySpecial or his input https://git.envs.net/NobodySpecial/whoami
- Thanks to Madaidan for his input https://madaidans-insecurities.github.io
- **Special Thanks to LiJu09 for helping with the Light theme of the website** https://github.com/LiJu09
- Thanks to the people at the various few commercial entities who do take privacy seriously
- Thanks to the whole open-source community and especially the Linux community
- Thanks to the many researchers, journalists, lawyers, and individuals referenced in this guide for their various research and projects
- **Special Thanks to Edward Snowden and who inspired me to write this guide (buy and read his book please https://en.wikipedia.org/wiki/Permanent_Record_(autobiography)** [Wikiless] [Archive.org]**)**

Appendix A: Windows Installation

This is the Windows 10 installation process that should be valid for any Windows 10 install within this guide.

Installation:

DO NOT CONNECT WINDOWS TO ANY NETWORK DURING THE INSTALLATION PROCESS (This will allow us to create a Local Account and not use a Microsoft account and it will also prevent any telemetry from being sent out during the install process).

- Click "Install Now"
- Select "I don't have a product key"
- Select the flavor you want:
    - Host OS: Use
        - You intend to use Plausible Deniability: Windows Home
        - You do not intend to use Plausible Deniability: Windows Pro
    - VM OS: Use Windows Pro or Windows Pro N
- Select Custom
- Storage:
    - If this is a simple OS installation (Host OS with Simple Encryption) or VM without encryption, **select the whole disk** and proceed with installation (skip next step).
    - If this is part of a plausible deniability encryption setup on the Host OS:
        - If you are installing Windows for the first time (Hidden OS):
            - Delete the current partitions
            - Create a First partition with at least 50GB of disk space (about a third of the total disk space).
            - Create a Second partition with the remaining two thirds of the total disk space.
        - If you are installing Windows for the second time (Decoy OS):
            - Do not Delete the current partitions

        - Install Windows on the first partition you created during the first install.
    - Proceed with the install in the First partition
- Start the install process
- Select the Region "United Kingdom"
- Skip the additional Keyboard Layout
- Select "I don't have internet"
- Select "Continue with limited setup"
- Create a username of your choice.
- Use a password of your choice.
- Select all 3 security questions and answer whatever you want (not real data).
- Do not use Online Speech Recognition
- Do not let app use your location
- Do not enable "find my device"
- Only send "required diagnostic data"
- Do not improve Inking and Typing
- Do not get any improved tailored experience.
- Do not let apps use Advertising ID
- Select "Now" at the Cortana prompt

Privacy Settings:

- When the install is finished, get into Settings > Privacy and do the following:
    - General: All Off
    - Speech: Off
    - Inking and Typing: Off
    - Diagnostic: Required level at off, options on OFF, **Delete your data**, frequency set to Never
    - Activity History: all Off and Clear the history
    - Location, all Off (change button) and clear it
    - Camera: Disable it (change button)
    - Microphone: Disable it (change button)
    - Voice Activation: All Off
    - Notification: Disable it (change button)
    - Account info: Disable it (change button)
    - Contact info: Disable it (change button)
    - Calendar access: Disable it (change button)
    - Phone calls: Disable it (change button)
    - Call History: Disable it (change button)
    - E-mail: Disable it (change button)
    - Tasks: Disable it (change button)
    - Messaging: Disable it (change button)
    - Radios: Disable it (change button)
    - Other devices: Set to Off
    - Background Apps: Disable it (change button)
    - App Diagnostics: Disable it (change button)
    - Documents: Disable it (change button)
    - Pictures: Disable it (change button)
    - Videos: Disable it (change button) and set to off
    - File system: Disable it (change button)
- Disable File Indexing by going into the "Indexing Options" (Go into Windows 10 Control Panel, Switch the view to "Large Icons" and select Indexing Options.
    - Modify the list and remove all locations.
    - Go into Advanced and click Rebuild.
- (Host OS only) Disable Bluetooth in the settings:

    - Go into Settings
    - Go into Devices
    - Select Bluetooth and turn it off
- (Host OS Only) Tape the Webcam and Microphone anyway for extra paranoia.
- (Host OS Only) Go into Settings > Network & Internet > Wi-Fi and Enable Random Hardware Address.

Appendix B: Windows Additional Privacy Settings

As written earlier in this guide and as noted by Privacytools.io[419], Windows 10 is a privacy nightmare. And disabling everything during and after the installation using the settings available to you is not enough. The amount of telemetry data collected by Microsoft is staggering and could defeat your attempts at keeping secrets. You will need to download and use a couple of utilities to (hopefully) force Windows 10 into not sending data back to Microsoft.

Here are the steps in details:

- **DO NOT EVER USE A MICROSOFT ACCOUNT TO LOG IN: If you are, you should be re-installing this Windows Machine without connecting to a network and use a local account instead.**

Do these steps from a different computer to not connect Windows 10 to the internet before those settings are applied. You can download and copy those to the USB key (for transfer onto a Windows 10 fresh installation) or if it is a VM, you can transfer them to the VM within Virtualbox (VM Settings > General > Advanced > Drag n Drop > Enable Host to Guest).

- Download and install W10Privacy from https://www.w10privacy.de/english-home/ [Archive org]
    - Open the app as Administrator (right click > more > run as administrator)
    - Check all the recommended (Green) settings and save.
    - Optional but recommended (but could break things, use at your own risk), also check the orange/red settings, and save.
    - Reboot
- Download and run WindowsSpyBlocker from https://crazymax.dev/WindowsSpyBlocker/download/ [Archive.org]
    - Type 1 and go into Telemetry
    - Type 1 and go into Firewall
    - Type 2 and add Spy Rules
    - Reboot
- Go back one last time Settings > Privacy > Diagnostic and Delete all Data.

These measures added to the settings during installation should be hopefully sufficient to prevent Microsoft from snooping on your OS.

You will need to update and re-run W10Privacy and WindowsSpyBlocker frequently and after any Windows update as they tend to silently re-enable telemetry using those updates.

Appendix C: Windows Installation Media Creation

These are the steps to create a Windows 10 (21H1) Installation Media using this tool and instructions:

https://www.microsoft.com/en-us/software-download/windows10 [Archive.org]

- Download the tool and execute it from your Download folder.
- Agree to the terms
- Select the process to Create and installation Media.
- Select Windows 10 64 Bits edition with the language of your choice.
- Pick which process you want:
    - If installing on a physical computer: Select USB Flash Drive
    - If installing on a Virtual Machine: Select ISO file and save it.

[419] Privacytools.io, Operating Systems https://privacytools.io/operating-systems/ [Archive.org]

- Proceed

Appendix D: Using System Rescue to securely wipe an SSD drive.

These instructions are valid for all Operating Systems:

- System Rescue:
  - Create a System Rescue USB disk following these instructions https://www.system-rescue.org/Installing-SystemRescue-on-a-USB-memory-stick/ [Archive.org] (download the ISO and write to an USB stick with Rufus).
  - Disable Secure Boot in your BIOS/UEFI settings and change the boot order to the USB disk (System Rescue bootloader is not signed and will not boot with secure boot enabled).
  - Follow the instructions to change the keyboard layout by typing "stkmap".
  - (optional) Run startx afterward to start a graphical environment.
- SATA SSD:
  - (If you ran startx) Open a terminal
  - ATA Secure Erase:
    - Follow one of these tutorials
      - https://wiki.archlinux.org/index.php/Solid_state_drive/Memory_cell_clearing [Archive org]
      - https://ata.wiki.kernel.org/index.php/ATA_Secure_Erase [Archive org]
      - https://tinyapps.org/docs/wipe_drives_hdparm.html [Archive org]
  - ATA Sanitize:
    - Follow this tutorial https://tinyapps.org/docs/ata_sanitize_hdparm.html [Archive org]
- NVMe SSD:
  - (If you ran startx) Open a terminal
  - Follow one of these tutorials:
    - https://wiki.archlinux.org/index.php/Solid_state_drive/Memory_cell_clearing [Archive.org]
    - https://tinyapps.org/docs/nvme-secure-erase.html [Archive org]
    - https://tinyapps.org/docs/nvme-sanitize.html [Archive.org]

Appendix E: Clonezilla

- Get Clonezilla by just following these instructions: https://clonezilla.org/liveusb.php [Archive.org] (I recommend the Alternative version AMD64 that should work with most recent laptops)
- Boot from Clonezilla
- Follow these steps to make a backup: https://clonezilla.org/show-live-doc-content.php?topic=clonezilla-live/doc/01_Save_disk_image [Archive.org]
  - **If you are backing up a disk with simple Encryption, encryption of the backup is not required since you are backing up an already encrypted disk but you can still encrypt the backup anyway if you want additional security (and slower backup).**
  - **If you intend to back-up a device with plausible deniability encryption, I strongly advise against it as this backup image could be used to prove the existence of the hidden volume using forensics techniques as explained earlier. Do not make an image backup of the partition containing your hidden OS.**
- You are done, if you need to restore, follow these instructions: https://clonezilla.org/show-live-doc-content.php?topic=clonezilla-live/doc/02_Restore_disk_image [Archive.org]

Each backup could take a while depending on the speed of your laptop and the speed of your external drive. In my experience, expect about 1 hour per backup depending on the drive size and the write speed of your backup media (my tests were done backing up 256GB SSDs on a USB 3.0 7200rpm HDD).

Appendix F: Diskpart

Diskpart is a Windows utility that can be used to perform various operations on your hard drive. In this case we will use Diskpart to show the Disk ID but also to change it if necessary.

This could be needed if you restore a backup on a new HDD/SSD that has an ID that differs from the one backed up and Windows could refuse to boot.

Diskpart can be run from any Windows environment using a command prompt. This includes recovery disks created by utilities such as Macrium Reflect, any Windows Installation media, EaseUS Todo Free rescue disks.

- **Displaying the disk ID**
  - Run Diskpart to enter the Diskpart utility
  - Issue the ```list disk``` command to list the disks
  - Issue the ```sel disk x``` (replace x with your system disk) to select your system disk
  - Issue the ```detail disk``` to show the details of this disk
  - Take note of the disk ID (this should be done BEFORE backing up your disks).
- **Changing the disk ID**
  - This step should only be done if, after restoring a full disk backup to a new hard drive, Windows refuses to boot
  - Issue the same commands as above on the target new disk
  - Issue in addition the command ```uniqueid disk id=02345678``` (where you replace the id by the one you noted before)

Appendix G: Safe Browser on the Host OS

If you can use Tor:

This guide will **only recommend** using Tor browser within the host OS because it has the best protections by default. The only other acceptable option in my opinion would be to use Brave Browser with a Tor tab **but keep in mind that Brave themselves recommend the use of Tor Browser if you feel your safety depends on being anonymous[420]: "If your personal safety depends on remaining anonymous, we highly recommend using Tor Browser instead of Brave Tor windows. ".**

This Browser on the host OS will only be used to download various utilities and will never be used for actual sensitive activities.

- Download and install Tor Browser according to the instructions from https://www.torproject.org/download/ [Archive org]
- Open Tor Browser
- Click the little shield Icon and select your Security level (see https://tb-manual.torproject.org/security-settings/ [Archive.org] for details):
  - Standard
  - Safer **(my recommended setting)**
  - Safest (this will have Javascript disabled on all websites and while increasing your security, it might reduce your anonymity and make your browsing experience quite unpleasant on many non-static websites).

If you are experiencing issues connecting to Tor due to Censorship or Blocking, you might consider using Tor bridges as explained here: https://bridges.torproject.org/ [Archive.org]

Use this browser for all the next steps within the host OS unless instructed otherwise.

[420] Brave Support, What is a Private Window with Tor? https://support.brave.com/hc/en-us/articles/360018121491-What-is-a-Private-Window-with-Tor- [Archive.org]

If you cannot use Tor:

Because it is too dangerous/risky/suspicious. I would recommend as a last resort using Firefox, Ungoogled-Chromium, or Brave only using Private Windows for now.

See Appendix P: Accessing the internet as safely as possible when Tor and VPNs are not an option before continuing.

Only do this from a different safe public Wi-Fi every time (See Find some safe places with decent public Wi-Fi) and using a long-range connection (See Appendix Q: Using long range Antenna to connect to Public Wi-Fis from a safe distance:).

Clean all the data from the browser after each use.

Use this method for all the next steps within the host OS unless instructed otherwise.

Appendix H: Windows Cleaning Tools

In this guide I will recommend two third native tools and two third party tools:

- Native Tools:
  - Windows 10 Disk Cleanup Utility: https://support.microsoft.com/en-us/windows/disk-cleanup-in-windows-10-8a96ff42-5751-39ad-23d6-434b4d5b9a68 [Archive.org]

    This tool will cleanup a bunch of things natively. It is not enough and I instead recommend using third party tools below to clean more stuff. PrivaZer for instance will use the disk cleanup utility directly itself and BleachBit will use its own mechanisms.

  - Windows 10 Optimize Utility (Defrag on HDD Drives): https://support.microsoft.com/en-us/windows/defragment-your-windows-10-pc-048aefac-7f1f-4632-d48a-9700c4ec702a [Archive.org]

    For security, this tool is very useful on SSD drives at this "Optimize" function will in fact force a Disk wide Trim operation to occur. This will most likely be more than enough to make sure any deleted data that was not trimmed before for any reason will be this time. Deleted data with Trim is very unlikely to be recovered as explained before in this guide.

- Third Party Tools:
  - The open-source utility BleachBit https://www.bleachbit.org/ [Archive org]
  - The closed-source utility PrivaZer https://privazer.com/ [Archive.org]

Personally, I prefer PrivaZer because it has more customization and smarter features but I would understand if you do not trust them and prefer open-source software in which case I would recommend BleachBit which offers a bit less customization but similar functionalities.

Both these tools can be used for cleaning many things such as:

- The Windows USN journal which stores plenty of information[421].
- The Windows System Resource Usage Monitor (SRUM)[422].
- Various histories of various programs (such as the recent lists).
- Various logs
- The free (unallocated) space of your hard drive[423].
- Secure deletion of files
- Secure wiping of USB drives

---

[421] Medium.com, The Windows USN Journal https://medium.com/velociraptor-ir/the-windows-usn-journal-f0c55c9010e [Archive org]

[422] Medium.com, Digging into the System Resource Usage Monitor (SRUM) https://medium.com/velociraptor-ir/digging-into-the-system-resource-usage-monitor-srum-afbadb1a375 [Archive.org]

[423] SANS, Timestamped Registry & NTFS Artifacts from Unallocated Space https://www.sans.org/blog/timestamped-registry-ntfs-artifacts-from-unallocated-space/ [Archive.org]

Both these utilities can delete files and can overwrite the free space after deletion to improve secure deletion even on SSD drives. Remember this can reduce the lifespan of your SSD drives a bit.

Appendix I: Using ShredOS to securely wipe an HDD drive:

There are several utilities that are recommend (like the old unmaintained DBAN[424]) or System Rescue CD (https://www.system-rescue.org/ [Archive org]) for this but personally, I will recommend the use of ShredOS.

Feel free do go with DBAN instead if you want (using this tutorial: https://www.lifewire.com/how-to-erase-a-hard-drive-using-dban-2619148 [Archive.org]), the process is basically the same but will not work out of the box with UEFI laptops.

If you want to go with System-Rescue, just head to their website and follow the instructions.

Windows:

- Download ShredOS from https://github.com/PartialVolume/shredos.2020.02 [Archive org]
- Unzip the ISO file
- Download Rufus from https://rufus.ie/ [Archive.org]
- Launch Rufus
- Select the ShredOS IMG file
- Write it to an USB key
- When done, reboot and boot the USB key (you might have to go into your BIOS settings to change the boot order for this).
- Follow the instructions on screen

Linux:

- Follow instructions on https://github.com/PartialVolume/shredos.2020.02 [Archive.org]
- Reboot and boot the USB key
- Follow the instructions on screen

Appendix J: Manufacturer tools for Wiping HDD and SSD drives:

Always check your laptop BIOS/UEFI for native utilities first.

Be sure to use the right wipe mode for the appropriate disk. Wipe and Passes are for HDD drives. There are specific options for SSD drives (such as ATA Secure Erase or Sanitize).

Unfortunately, most of these tools are Windows only.

Tools that provide a boot disk for wiping from boot:

- SanDisk DashBoard: https://kb.sandisk.com/app/answers/detail/a_id/15108/~/dashboard-support-information [Archive.org]
- Seagate SeaTools: https://www.seagate.com/support/downloads/seatools/ [Archive org]
- Samsung Magican: https://www.samsung.com/semiconductor/minisite/ssd/download/tools/ [Archive org]
- Kingston SSD Manager: https://www.kingston.com/unitedstates/en/support/technical/ssdmanager [Archive.org]
- Lenovo:
    - Most likely native utility available within the BIOS/UEFI, please check
    - Drive Erase Utility: https://support.lenovo.com/us/en/downloads/ds019026-thinkpad-drive-erase-utility-for-resetting-the-cryptographic-key-and-erasing-the-solid-state-drive-thinkpad [Archive.org]
- Crucial Storage Executive: https://www.crucial.com/support/storage-executive [Archive.org]
- Western Digital Dashboard: https://support.wdc.com/downloads.aspx?p=279 [Archive org]
- HP: Follow instructions on https://store.hp.com/us/en/tech-takes/how-to-secure-erase-ssd [Archive.org]
- Transcend SSD Scope: https://www.transcend-info.com/Support/Software-10/ [Archive.org]
- Dell:

[424] DBAN, https://dban.org/ [Archive.org]

- Most likely native utility available within the BIOS/UEFI, please check https://www.dell.com/support/kbdoc/en-us/000134997/using-the-dell-bios-data-wipe-function-for-optiplex-precision-and-latitude-systems-built-after-november-2015?lwp=rt [Archive.org]

Tools that provide only support from running OS (for external drives).

- Toshiba Storage Tools: https://www.toshiba-storage.com/downloads/ [Archive.org]

Appendix K: Considerations for using external SSD drives

I do not recommend using external SSDs due to the uncertainty about their support for Trim, ATA Secure Erase and Sanitize options through USB controllers. Instead, I recommend using external HDD disks which can be cleaned/wiped safely and securely without hassle (albeit much slower than SSD drives).

Please do not buy or use gimmicky self-encrypting devices such as these:
https://syscall.eu/blog/2018/03/12/aigo_part1/ [Archive.org]

Some might be very efficient[425] but many are gimmicky gadgets.

If you really want to use an external SSD drive for sensitive storage:

- Please consider the support for:
  - Trim operations and ATA/NVMe secure erase operations from your Laptop USB controller.
  - Trim operations and ATA/NVMe secure erase operations from your USB SSD disk itself.
- Always use full disk encryption on those disks
- **Use the manufacturer provided tools to securely erase them if possible (see Appendix K: Considerations for using external SSD drives).**
- Consider manually wiping data on them after use by doing a full decryption/encryption or filling them completely with random data.

So how to check if your external USB SSD supports Trim and other ATA/NVMe operations from your Host OS?

Windows:

Trim Support:

It is possible Windows will detect your external SSD properly and enable Trim by default. Check if Optimize Works using the Windows Native disk utility as explained in the internal SSD section of Windows.

ATA/NVMe Operations (Secure Erase/Sanitize):

Use the manufacturer provided tools to check and perform these operations … It is pretty much the only way to be sure it is not only supported but actually works. Some utilities can tell you if it is supported or not like CrystalDiskInfo[426] but will not actually check if it is working. See Appendix J: Manufacturer tools for Wiping HDD and SSD drives.

If it does not work. Just decrypt and re-encrypt the whole drive or fill up the free space as instructed in the guide. There is no other way AFAIK. Besides booting up a System Rescue Linux CD and see the next section.

Linux:

Trim Support:

Follow this good tutorial: https://www.glump.net/howto/desktop/enable-trim-on-an-external-ssd-on-linux [Archive.org]

[425] NYTimes, Lost Passwords Lock Millionaires Out of Their Bitcoin Fortunes
https://www.nytimes.com/2021/01/12/technology/bitcoin-passwords-wallets-fortunes.html [Archive.org]

[426] CrystalDiskInfo https://crystalmark.info/en/software/crystaldiskinfo/ [Archive.org]

ATA/NVMe Operations (Secure Erase/Sanitize):

It is not "recommended". Please read the disclaimers here https://ata.wiki.kernel.org/index.php/ATA_Secure_Erase [Archive.org] **and here https://wiki.archlinux.org/index.php/Solid_state_drive/Memory_cell_clearing** [Archive.org]

But this seems to be based on anecdotal experiences. So, if you are sure your external SSD supports Trim (see vendor documentation). You could just **try at your own risk** to use nvme-cli or hdparm to issue secure erases.

See also this tutorial https://code.mendhak.com/securely-wipe-ssd/ [Archive org]

Your mileage may vary. Use at your own risk.

MacOS:

Trim Support:

According to Apple Documentation[405], Trim is supported on APFS (asynchronously) and HFS+ (through period trim or first-aid).

So, if it is supported (and enabled on your external SSD), you should be able to issue a Trim on a non-APFS drive using Disk Utility and First Aid which should issue a Trim.

If your disk supports it but it is not enabled in MacOS. You could try issuing a "sudo trimforce enable" command from the Terminal and see if it enables Trim on your external SSD. And then again check the first aid command if it is not APFS (see this Tutorial for info https://www.lifewire.com/enable-trim-for-ssd-in-os-x-yosemite-2260789 [Archive org])

If it does not work, I am not aware of any reliable method to enable TRIM besides the commercial utility Trim Enabler here https://cindori.org/trimenabler/ [Archive.org] which claims support for external drives.

ATA/NVMe Operations (Secure Erase/Sanitize):

I am not aware of any method of doing so reliably and safely on MacOS. So, you will have to try one of these options:

- Use a bootable System Rescue USB Linux to do it
- Just decrypt and re-encrypt the drive using Disk Utility or Veracrypt
- Fill up the free space of the disk using the Linux method (dd)

Appendix L: Creating a mat2-web guest VM for removing metadata from files

Download the latest Debian testing amd64 netinst ISO from https://www.debian.org/CD/netinst/ [Archive.org]

(Get testing to get the latest mat2 release, stable is a few versions back)

This is very lightweight and I recommend you do it from a VM (VM inside a VM) to benefit from Whonix Tor Gateway. While it is possible to put this VM directly behind a Whonix Gateway. Whonix will not easily (AFAIK) allow communications between VMs on its network by default.

You could also just leave it on Clearnet during the install process and then leave it on the Host Only network later.

Or install it from a VM within a VM then move it the host OS for Host Only usage.

- Create a new machine with any name like mat2
- Select Linux as Type
- Select Debian (64-bit) as Version
- Leave the default options and click create
- Select the VM and click Settings
- Select System and disable the Floppy disk on the Motherboard tab
- Select the Processor tab and enable PAE/NX
- Select Audio and disable Audio
- Select USB and disable the USB controller

- Select Storage and select the CD drive to mount the Debian Netinst ISO
- Select Network and Attach to NAT
- Launch the VM
- Select Install (not Graphical install)
- Select Language, Location and Keyboard layout as you wish
- Wait for network to configure (automatic DHCP)
- Pick a name like "Mat2"
- Leave the domain empty
- Set a Root password as you wish (preferably a good one still)
- Create a new user and password as you wish (preferably a good one still)
- Select the Time Zone of your choice
- Select Guided - Use entire disk
- Select the only ask available
- Select All files in one partition
- Confirm and write changes to disk
- Select NO to scan any other CD or DVD
- Select any region and any mirror of your choice and leave proxy blank
- Select no to participate in any survey
- Select only System Standard Utilities (uncheck everything else)
- Select Yes to install GRUB bootloader
- Select /dev/sda and continue
- Complete the install and reboot
- Login with your user or root (you should never use root directly as a best security practice but in this case, I think it is “okay")
- Update your install by running ```su apt upgrade``` (but it should be upgraded since it is a net install)
- Install the necessary packages for mat2 by running ```su apt install ffmpeg uwsgi python3-pip uwsgi-plugin-python3 librsvg2-dev git mat2 apache2 libapache2-mod-proxy-uwsgi```
- Go to the /var/www directory by running ```cd /var/www/```
- Clone mat2-web from the mat2-web repository by issuing ```git clone https://0xacab.org/jvoisin/mat2-web.git```
- Create a directory for uploads by running ```mkdir ./mat2-web/uploads/```
- Give permissions to Apache2 to read the files by running ```chown -R www-data:www-data ./mat2-web```
- Enable apache2 uwsgi proxy by running ```/usr/sbin/a2enmod proxy_uwsgi```
- Upgrade pip by running ```python3 -m pip install pip --upgrade```
- Install some python modules by running ```python3 -m pip install flasgger pyyaml flask-restful flask cerberus flask-cors jinja2```
- Move to the config directory of mat2 by running ```cd /var/www/mat2-web/config/```
- Copy the apache2 config file to etc by running ```cp apache2.config /etc/apache2/sites-enabled/apache2.conf```
- Remove the default config file by running ```rm /etc/apache2/sites-enabled/000-default.conf```
- Edit the apache2 config file provided by mat2-web by running ```nano /etc/apache2/sites-enabled/apache2.conf```
- Remove the first line ```Listen 80```
- Change the uwsgi path from ```/var/www/mat2-web/mat2-web.sock``` to ```/run/uwsgi/uwsgi.sock``` and save/exit
- Copy the uwsgi config file to etc by running ```cp uwsgi.config /etc/uwsgi/apps-enabled/uwsgi.ini```
- Edit the uwsgi config file and change uid and guid to ```nobody``` and ```nogroup```
- Run ```chown -R 777 /var/www/mat2-web```
- Restart uwsgi by running ```systemctl restart uwsgi``` (there should be no errors)
- Restart apache2 by running ```systemctl restart apache2``` (there should be no errors)
- Now change the network settings of the VM to “Host Only Network’

- Reboot the VM
- Log into the VM and type ```ip a``` to note the IP address it was assigned.
- From the VM Host OS open a Browser and go to the IP of your Debian VM (for example http://192.168.1.55)
- You should now see a Mat2-Web website running smoothly
- Shutdown the Mat2 VM by running ```shutdown -h now```
- Take a Snapshot of the VM within Virtualbox
- Restart the Mat2 VM and you are ready to use Mat2-web to remove metadata from most files
- After use, shutdown the VM and revert to the snapshot to remove traces of the uploaded files
- This VM does not require any internet access unless you want to update it in which case you need to place it back on the NAT network and do the next steps.
- For updates of Debian, start the VM and run ```apt update``` followed by ```apt upgrade```
- For updates of mat2-web, go to /var/www/mat2-web and run ```git pull```
- After updates, shutdown, place it back on the Host Network, take a new snapshot, remove the previous one keeps going

You are done.

Now you can just start this small mat2 VM when needed, browse to it from your Guest VM and use the interface to remove any metadata from most files.

After each use of this VM, you should revert to the Snapshot to erase all traces.

Do not ever expose this VM to any network unless temporarily for updates. This web interface is not suitable for any direct external access.

Appendix M: BIOS/UEFI options to wipe disks in various Brands

Here are some links on how to securely wipe your drive (HDD/SSD) from the BIOS for various brands:

- Lenovo ThinkPads: https://support.lenovo.com/be/en/solutions/migr-68369 [Archive.org]
- HP (all): https://support.hp.com/gb-en/document/c06204100 [Archive.org]
- Dell (all): https://www.dell.com/support/kbdoc/en-us/000146892/dell-data-wipe [Archive.org]
- Acer (Travelmate only): https://us.answers.acer.com/app/answers/detail/a_id/41567/~/how-to-use-disk-sanitizer-on-acer-travelmate-notebooks [Archive.org]
- Asus: no option AFAIK except maybe for some ROG models.
- Gigabyte: no option AFAIK
- Honor: no option AFAIK
- Huawei: no option AFAIK

Appendix N: Warning about smartphones and smart devices

When conducting sensitive activities, remember that:

- You should not to bring your smartphone/smart devices with you (even turned off, unless you can remove the battery or are certain it is completely powered off).
- If you really must take them with you, you could consider the use of a faraday cage[427] bag to store your devices. There are many such faraday "signal blocking" bags available for sale and some of these have been studied[428] for their effectiveness. If you cannot afford such bags, you can probably achieve a "decent result" with one or several sheets of aluminum foil (as shown in the previously linked study).

[427] Wikipedia, Faraday Cage, https://en.wikipedia.org/wiki/Faraday_cage [Wikiless] [Archive.org]

[428] Edith Cowan University, A forensic examination of several mobile device Faraday bags & materials to test their effectiveness materials to test their effectiveness https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1165&context=adf [Archive.org]

    - Warning: consider that sensor data itself can also be reliably used to track you[429,430].
- Consider leaving your smart devices at home online and doing something (watching YouTube/Netflix or something similar) instead of taking them with you powered off. This will mitigate tracking efforts but also create digital traces that could indicate you were at home.

Note: Please do not consider commercial gimmicky all-in devices for anonymity. The only way to achieve proper opsec is by doing it yourself. See those examples to see why it is not a good idea:

- **Encrochat: https://en.wikipedia.org/wiki/EncroChat** [Wikiless] [Archive.org]
- **Sky ECC: https://en.wikipedia.org/wiki/Sky_ECC** [Wikiless] [Archive.org]

You should never rely on some external commercial service to protect your anonymity.

Appendix O: Get an anonymous VPN/Proxy

If you follow my advice, you will also need a VPN subscription but this time you will need an anonymous one that cannot be tied to you by the financial system. Meaning you will need to buy a VPN subscription with cash or a reasonably private crypto currency (Monero). You will later use this VPN to connect to the various services anonymously but never directly from your IP.

I only see two possible options for you to get an anonymous VPN/Proxy:

Cash/Monero-Paid VPN (preferred):

There are three VPN companies recommended by privacytools.io (https://privacytools.io/providers/vpn/ [Archive.org]) that accept cash payments: Mullvad, iVPN and ProtonVPN.

Personally, I would recommend Mullvad due to personal experience.

I would not recommend ProtonVPN as much because they do require an e-mail for registration unlike Mullvad and iVPN.

How does this work?

- Access the VPN website with a Safe Browser (see Appendix G: Safe Browser)
- Go to iVPN or Mullvad website and create a new Account ID (on the login page).
- This page will give you an account ID, a token ID (for payment reference) and the details where to send the money by post.
- Send the required cash amount for the subscription you want in a sealed postal envelope to their offices, including a paper with the Token ID without a return address or pay with Monero. If they do not accept Monero but do accept BTC, consider Appendix Z: Paying anonymously online with BTC
- Wait for them to receive the payment and enable your account (this can take a while).
- Open Tor Browser.
- Check your account status and proceed when your account is active.

For extra-security consider:

- Wearing gloves while manipulating anything to avoid leaving fingerprints[431] and touch DNA[432].
- Do not use any material/currency that was manipulated by someone that can be related to you in any way.
- Do not use currency you just got from an ATM that could record dispensed bills serial numbers.
- Be careful if you print anything that it is not watermarked by your printer (See Printing Watermarking).

---

[429] arXiv, Deep-Spying: Spying using Smartwatch and Deep Learning https://arxiv.org/abs/1512.05616 [Archive.org]

[430] Acm.org, Privacy Implications of Accelerometer Data: A Review of Possible Inferences https://dl.acm.org/doi/pdf/10.1145/3309074.3309076 [Archive org]

[431] YouTube, Fingerprinting Paper - Forensic Education https://www.youtube.com/watch?v=sO98kDLkh-M [Invidious]

[432] Wikipedia, Touch DNA, https://en.wikipedia.org/wiki/Touch_DNA [Wikiless] [Archive.org]

- Do not lick the envelope or the stamps[433] if you use them to avoid leaving DNA traces.
- Make sure there are no obvious DNA traces in or on the materials (like hairs).
- Consider doing the whole operation outdoor to reduce the risks residual DNA traces from your environment or yourself contaminating the materials.

Do not in any circumstance use this new VPN account unless instructed or connect to that new VPN account using your known connections. This VPN will only be used later in a secure way as we do not trust VPN providers "no logging policies". This VPN provider should ideally never know your real origin IP (your home/work one for instance).

Self-hosted VPN/Proxy on a Monero/Cash-paid VPS (for skilled users familiar with Linux):

The other alternative is setting up your own VPN/Proxy using a VPS (Virtual Private Server) on a hosting platform that accepts Monero (recommended).

This will offer some advantages as the chances of your IP being blacklisted somewhere are lower than known VPN providers.

This does offer some disadvantage as Monero is not perfect as explained earlier in this guide and some global adversaries could maybe still track you. You will need to get Monero from an Exchange using the normal financial system and then pick a hosting (list here https://www.getmonero.org/community/merchants/#exchanges [Archive.org])

Do not in any circumstance use this new VPS/VPN/Proxy using your known connections. Only access it through Tor using Whonix Workstation for instance (this is explained later). This VPN will only be used later within a Virtual Machin over the Tor Network in a secure way as we do not trust VPN providers "no logging policies". This VPN provider should never know your real origin IP.

Please see Appendix A1: Recommended VPS hosting providers

VPN VPS:

There are plenty of tutorials on how to do this like this one https://proprivacy.com/vpn/guides/create-your-own-vpn-server [Archive.org]

Socks Proxy VPS:

This is also an option obviously if you prefer to skip the VPN part.

It is probably the easiest thing to set-up since you will just use the SSH connection you have to your VPS and no further configuration should be required.

Here are a few tutorials on how to do this very quickly:

- (Windows/Linux/MacOS) https://linuxize.com/post/how-to-setup-ssh-socks-tunnel-for-private-browsing/ [Archive org]
- (Windows/Linux/MacOS) https://www.digitalocean.com/community/tutorials/how-to-route-web-traffic-securely-without-a-vpn-using-a-socks-tunnel [Archive.org]
- (Windows) https://www.forwardproxy.com/2018/12/using-putty-to-setup-a-quick-socks-proxy/ [Archive.org]
- (Linux/MacOS) https://ma.ttias.be/socks-proxy-linux-ssh-bypass-content-filters/ [Archive.org]

Here is my basic tutorial:

Linux/MacOS:

Here are the steps:

- Get your anonymous VPS set-up
- From a terminal, SSH to your server by running: ```ssh -i ~/.ssh/id_rsa -D 8080 -f -C -q -N username@ip_of_your_server```

[433] TheDNAGuide, DNA from Postage Stamps or Hair Samples? Yeeesssss..... https://www.yourdnaguide.com/ydgblog/dna-hair-samples-postage-stamps [Archive.org]

- Configure your browser to use localhost:8080 as a Socks Proxy for Browsing
- Done!

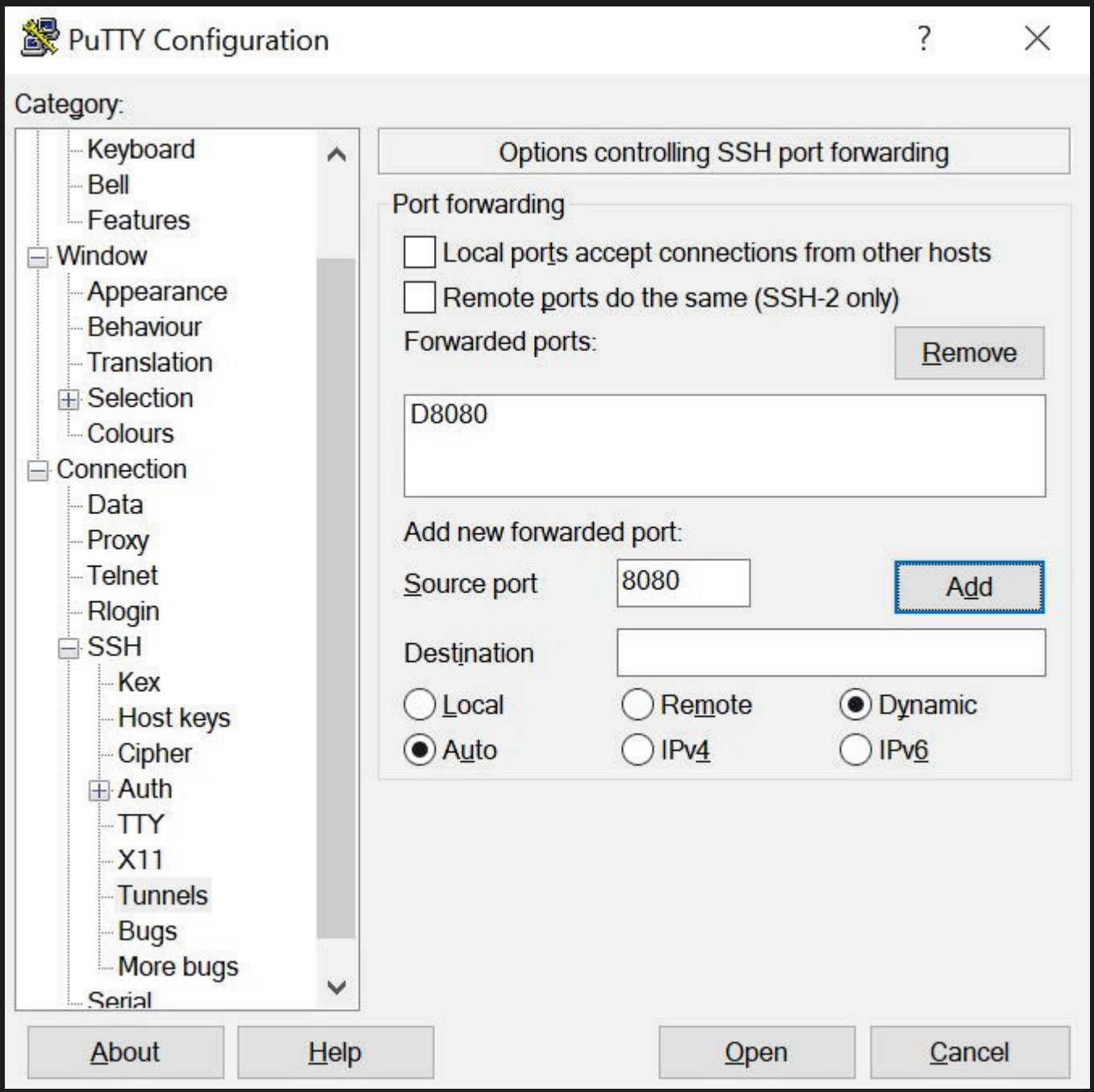
Explanation of arguments

- -i: The path to the SSH key to be used to connect to the host
- -D: Tells SSH that we want a SOCKS tunnel on the specified port number (you can choose a number between 1025 and 65536)
- -f: Forks the process to the background
- -C: Compresses the data before sending it
- -q: Uses quiet mode
- -N: Tells SSH that no command will be sent once the tunnel is up

Windows:

Here are the steps:

- Get your anonymous VPS set-up
- Download and install Putty from https://www.putty.org/ [Archive.org]
- Set the following Options in Putty and connect to your server



- Connect to your VPS using those settings
- Configure your Browser to use localhost:8080 as a Socks Proxy
- Done!

Appendix P: Accessing the internet as safely as possible when Tor and VPNs are not an option

USE EXTREME CAUTION: THIS IS HIGHLY RISKY.

There might be worst case situations where using Tor and VPNs are not possible due to extensive ad active censorship, or blocking. Even when using Tor Bridges (see Appendix X: Using Tor bridges in hostile environments)

Now, there might also be situations where simply using Tor or a VPN alone could be suspicious and could be dangerous for your safety. If this is case, you could be on a very hostile environment where surveillance and control is high.

But you still want to do something anonymously without disclosing/leaking any information.

In that case my last resort recommendation is to connect safely **from a distance** to a Public Wi-Fi (See Find some safe places with decent public Wi-Fi) using your laptop and Tails "unsafe browser". See https://tails.boum.org/contribute/design/Unsafe_Browser/ [Archive.org].

In Tor usage alone is suspicious or risky, you should NOT allow Tails to try establishing a Tor connection at start-up by doing the following:

- At startup open the Additional Settings.
- Enable Unsafe Browser.
- Change the Connection from Direct to "Configure a Tor Bridge or Local Proxy"
- After Start-up, Connect to a safe Network
- When prompted, just quit the Tor Connection Wizard (to not establish a Tor connection)
- Start and use the Unsafe Browser

I would strongly recommend the use of a long-range "Yagi" type directional Antenna with an appropriate USB Wi-Fi Adapter. At least this will allow you to connect to public Wi-Fis from a "safe distance" but keep in mind that triangulation by a motivated adversary is still possible with the appropriate equipment. So, this option should not be used during long period of times (minutes at best). See Appendix Q: Using long range Antenna to connect to Public Wi-Fis from a safe distance.

Using Tails should prevent local data leaks (such as MAC addresses or telemetry) and allow you to use a Browser to get what you want (utilities, VPN account) before leaving that place as fast as possible.

You could also use the other routes (Whonix and Qubes OS without using Tor/VPN) instead of Tails in such hostile environments if you want data persistence but this might be riskier. I would not risk it personally unless there was absolutely no other option. If you go for this option, you will only do sensitive activities from a reversible/disposable VM in all cases. Never from the Host OS.

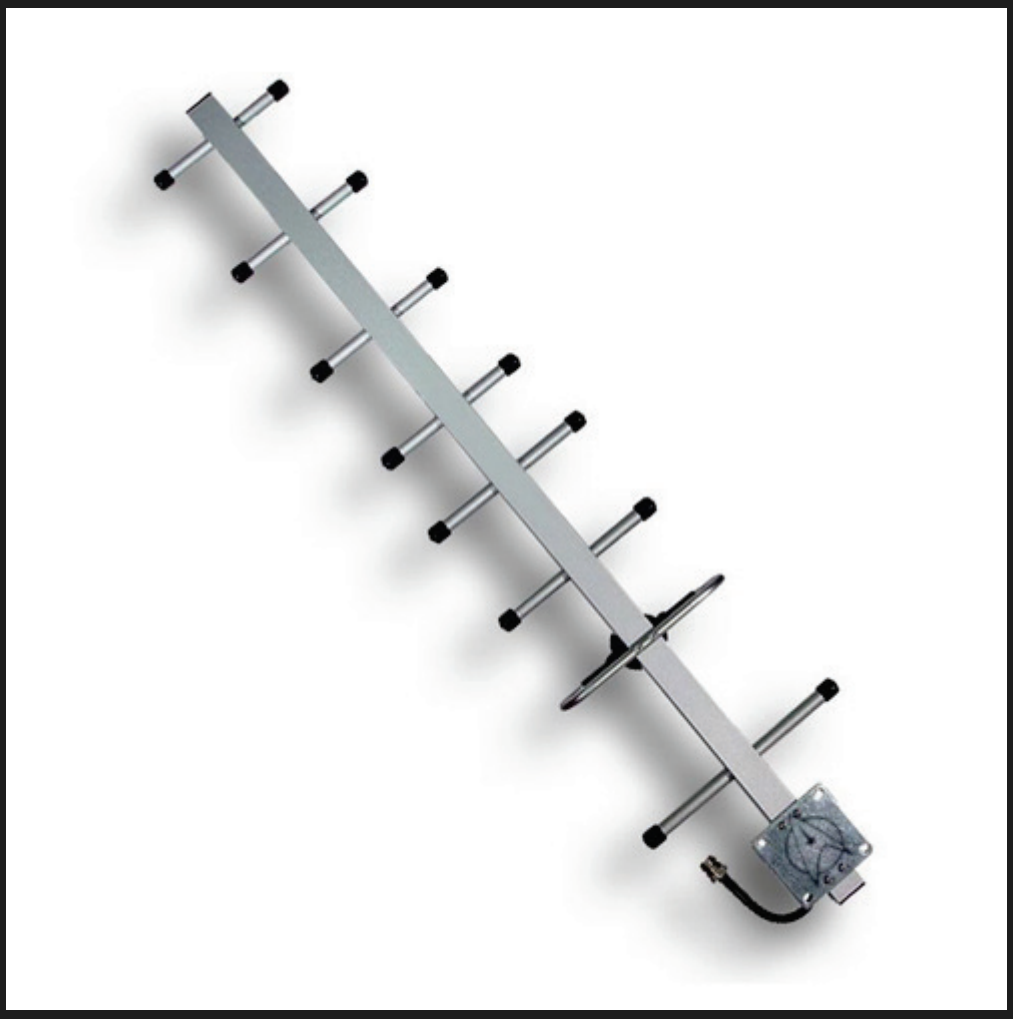
If you resort to this, please keep your online time as short as possible (minutes and not hours).

Be safe and extremely cautious. This is entirely at your own risk.

Consider reading this older but still relevant guide https://archive.flossmanuals.net/bypassing-censorship/index.html [Archive org]

Appendix Q: Using long range Antenna to connect to Public Wi-Fis from a safe distance:

It is possible to access/connect to remote distant Public Wi-Fis from a distance using a cheap directional Antenna that looks like this:



These antennas are widely available on various online shops for a cheap price (Amazon, AliExpress, Banggood …). The only issue is that they are not discrete and you might have to find a way to hide it (for instance in a Poster cardboard container in a Backpack). Or in a large enough Bag. Optionally (but riskier) you could even consider using it from your home if you have a nice Window view to various places where some Public Wi-Fi is available.

Such antennas need to be combined with specific USB adapters that have an external Antenna plug and sufficiently high power to use them.

Personally, I would recommend the AWUS036 series in the Alfa brand of adapters (see https://www.alfa.com.tw/ [Archive org]**).** But you could also go with some other brands if you want such as the TP-Link TL-WN722 (see https://www.tp-link.com/us/home-networking/usb-adapter/tl-wn722n/ [Archive.org]).

See this post for a comparison of various adapters: https://www.wirelesshack.org/best-kali-linux-compatible-usb-adapter-dongles.html [Archive.org] (Usually those antennas are used by Penetration Testers to probe Wi-Fis from a distance and are often discussed within the scope of the Kali Linux distribution).

The process is simple:

- Plug in and install your USB adapter on your Host OS.
- **Do not forget to randomize your MAC Address in case you bought this adapter online to prevent traceability (this is enabled by default in Tails).**
- Connect the Long-Range Antenna to the USB adapter (in place of the supplied one).
- Get to a convenient spot where you have a distant view on a place with a Public Wi-Fi available (this can be a rooftop for instance) but you could also imagine hiding the Antenna in some bag and just sit on a Bench somewhere.
- Point the Directional Antenna in the direction of the Public Wi-Fi.
- Connect to the Wi-Fi of your choice.

Do not forget tho that this will only delay a motivated adversary. Your signal can be triangulated easily by a motivated adversary in a matter of minutes once they reach the physical location of the Wi-Fi you're connecting to (for instance using a device such as AirCheck https://www.youtube.com/watch?v=8FV2QZ1BPnw [Invidious], also see their other products here https://www.netally.com/products/#wifi_s [Archive.org]). These products can easily be deployed on mobile units (in a Car for instance) and pinpoint your location in a matter of minutes.

Ideally this should "not be an issue" since this guide provides multiple ways of hiding your origin IP using VPNs and Tor. But if you are in the situation where VPN and Tor are not an option, then this could be your only security.

Appendix R: Installing a VPN on your VM or Host OS.

Download the VPN client installer of your cash paid VPN service and install it on Host OS (Tor over VPN, VPN over Tor over VPN) or the VM of your choice (VPN over Tor).

- Whonix Tutorial (should work with any VPN provider): https://www.whonix.org/wiki/Tunnels/Connecting_to_a_VPN_before_Tor [Archive.org] (use the Linux configurations below to get the necessary configuration files)
- Windows Tutorials:
  - Mullvad: https://mullvad.net/en/help/install-mullvad-app-windows/ [Archive org]
  - iVPN: https://www.ivpn.net/apps-windows [Archive.org]
  - ProtonVPN: https://protonvpn.com/support/protonvpn-windows-vpn-application/ [Archive.org]
- MacOS:
  - Mullvad: https://mullvad.net/en/help/install-and-use-mullvad-app-macos/ [Archive org]
  - IVPN: https://www.ivpn.net/apps-macos/ [Archive.org]
  - ProtonVPN: https://protonvpn.com/support/protonvpn-mac-vpn-application/ [Archive.org]
- Linux:
  - Mullvad: https://mullvad.net/en/help/install-mullvad-app-linux/ [Archive.org]
  - iVPN: https://www.ivpn.net/apps-linux/ [Archive.org]
  - ProtonVPN: https://protonvpn.com/support/linux-vpn-setup/ [Archive.org]

Important note: Tor does not support UDP and you should use TCP instead with the VPN client in the Tor over VPN cases (on the VMs).

In all cases you should set the VPN to start from boot and enable the "kill switch" if you can. This is an extra-step since this guide proposes solutions that all fall back on Tor network in case of VPN failure. Still recommended IMHO.

Here are some guides provided by the recommended VPN providers in this guide:

- Windows:
  - iVPN: https://www.ivpn.net/knowledgebase/general/do-you-offer-a-kill-switch-or-vpn-firewall/ [Archive org]
  - ProtonVPN: https://protonvpn.com/support/what-is-kill-switch/ [Archive org]
  - Mullvad: https://mullvad.net/en/help/using-mullvad-vpn-app/#killswitch [Archive.org]
- Whonix Workstation: Coming Soon, it is certainly possible but I did not find a suitable and easy tutorial yet. It is also worth remembering that if your VPN stops on Whonix, you will still be behind the Tor Network.
- MacOS:
  - Mullvad same as Windows, the option should be in the provided VPN client
  - iVPN same as Windows, the option should be in the provided VPN client
  - ProtonVPN same as Windows with the client, the option should be in the provided VPN client https://protonvpn.com/blog/macos-vpn-kill-switch/ [Archive.org]
- Linux:
  - Mullvad:
    - https://mullvad.net/en/help/wireguard-and-mullvad-vpn/ [Archive.org]
    - https://mullvad.net/en/help/linux-openvpn-installation/ [Archive.org]
  - ProtonVPN: https://github.com/ProtonVPN/linux-cli/blob/master/USAGE.md#kill-switch [Archive.org]
  - iVPN:

- https://www.ivpn.net/knowledgebase/linux/linux-wireguard-kill-switch/ [Archive.org]
- https://www.ivpn.net/knowledgebase/linux/linux-kill-switch-using-the-uncomplicated-firewall-ufw/ [Archive.org]

Appendix S: Check your network for surveillance/censorship using OONI

So, what is OONI? OONI stands for Open Observatory of Network Interference and is a sub-project of the Tor Project[257].

First OONI will allow you to check online for surveillance/censorship in your country just by looking at their Explorer that features test results from other people. This can be done here: https://explorer.ooni.org/

But these tests are limited and could not apply to your personal situation. If that is the case, you could consider running the OONI Probe yourself and running the tests yourself.

The problem obviously is that your network providers will be able to see those tests and your attempts at connecting to various services if the network is monitored. The other issue is that there are solutions to prevent OONI from working properly[434].

While this might not be important in a normal environment, this could put you at risk in a hostile environment. **So, running these tests can be risky.**

If you are in such a hostile environment where you suspect network activity is actively monitored and the simple fact of trying to access some resources can put you at risk, you should take some precautions before even attempting this:

- **Do not run the tests from your home/work network obviously.**
- **Do not run these tests from a known device or a smartphone but only for a secured OS on an ideally dedicated laptop.**
  - **You will not be able to do this from Tails as Tails will try to connect to Tor by default**
  - **You should only do this with the Qubes OS route or the Whonix Route of this guide after completing one of the routes.**
- **Only consider running these tests quickly from a Public Wi-Fi from a safe distance (see Appendix P: Accessing the internet as safely as possible when Tor and VPNs are not an option).**

The probe can be found here: https://ooni.org/install/ [Archive org] for various platforms (iOS, Android, Windows, MacOS, and Linux).

Appendix T: Checking files for malware

Integrity (if available):

Usually, integrity checks[435] are done using hashes of files (usually stored within checksum files). Older files could use CRC[436], more recently MD5[437] but those present several weaknesses (CRC, MD5[438]) that makes them unreliable for file integrity checks (which does not mean they are not still widely used in other contexts).

This is because they do not prevent Collision[439] well enough and could allow an adversary to create a similar but malicious file that would still produce in the same CRC or MD5 hash despite having a different content.

---

[434] GitHub, Mhinkie, OONI-Detection https://github.com/mhinkie/ooni-detection [Archive org]

[435] Wikipedia, File Verification https://en.wikipedia.org/wiki/File_verification [Wikiless] [Archive org]

[436] Wikipedia, CRC https://en.wikipedia.org/wiki/Cyclic_redundancy_check [Wikiless] [Archive org]

[437] Wikipedia, MD5 https://en.wikipedia.org/wiki/MD5 [Wikiless] [Archive.org]

[438] Wikipedia, MD5 Security https://en.wikipedia.org/wiki/MD5#Security [Wikiless] [Archive.org]

[439] Wikipedia, Collisions https://en.wikipedia.org/wiki/Collision_(computer_science) [Wikiless] [Archive.org]

For this reason, it is usually recommended to use SHA[440] based hashes and the most used is probably the SHA-2[441] based SHA256 for verifying file integrity. SHA is much more resistant to collisions[442] than CRC and MD5. And collisions with SHA256 or SHA512 are rare and hard to compute for an adversary.

If an SHA256 checksum is available from the source of the file, you should not hesitate to use it to validate the integrity of the file.

Obviously, this checksum should itself be authenticated/trusted and should be available from an authenticated/trusted source (obviously you should not trust a file just because it has a checksum attached to it alone).

In the case of this guide, the SHA256 checksums are available for each file including the PDFs but are also authenticated using a GPG signature allowing you to verify the authenticity of the checksum. This will bring us to the next section about authenticity.

So how to check checksums? (In this case SHA256 but you could change to SHA512

- Windows[443]:
  - Open a Command Prompt
  - Run ```certutil -hashfile filename.txt sha256``` (replace sha256 by sha1 or sha512 or md5)
  - Compare your result to one from a source you trust for that file
- MacOS[444]:
  - Open a Terminal
  - SHA: Run ```shasum -a 256 /full/path/to/your/file``` (replace 256 by 512 or 1 for SHA-1)
  - MD5: Run ```md5 /full/path/to/your/file```
  - Compare your result to one from a source you trust for that file
- Linux:
  - Open a Terminal
  - Run ```shasum /full/path/to/your/file``` (replace shasum by sha256sum, sha512sum or md5sum)
  - Compare your result to one from a source you trust for that file

Remember that checksums are just checksums. Having a matching checksum does not mean the file is safe.

Authenticity (if available):

Integrity is one thing. Authenticity is another thing. This is a process where you can verify some information is authentic and from the expected source. This usually done by signing information (using GPG[445] for instance) using public key cryptography[446].

Signing can serve both purposes and allow you to check for both integrity and authenticity.

If available, you should always verify signatures of files to validate their authenticity.

In essence:

- Install GPG for your OS:
  - Windows: gpg4win (https://www.gpg4win.org/ [Archive.org])
  - MacOS: GPGTools (https://gpgtools.org/ [Archive.org])
  - Linux: It should be pre-installed in most distributions

---

[440] Wikipedia, SHA https://en.wikipedia.org/wiki/Secure_Hash_Algorithms [Wikiless] [Archive.org]

[441] Wikipedia, SHA-2 https://en.wikipedia.org/wiki/SHA-2 [Wikiless] [Archive.org]

[442] Wikipedia, Collision Resistance https://en.wikipedia.org/wiki/Collision_resistance [Wikiless] [Archive.org]

[443] GnuPG Gpg4win Wiki, Check integrity of Gpg4win packages https://wiki.gnupg.org/Gpg4win/CheckIntegrity [Archive.org]

[444] Medium.com, How to verify checksum on Mac https://medium.com/@EvgeniIvanov/how-to-verify-checksum-on-mac-988f166b0c4f [Archive.org]

[445] Wikipedia, GPG https://en.wikipedia.org/wiki/GNU_Privacy_Guard [Wikiless] [Archive.org]

[446] Wikipedia, Public-Key Cryptography https://en.wikipedia.org/wiki/Public-key_cryptography [Wikiless] [Archive.org]

- Download the Signature key from a trusted source. If someone is not giving you a key directly, you should check for multiple versions on other websites to confirm you are using the right key (GitHub, GitLab, Twitter, Keybase, Public Keys Servers…).
- Import the trusted key (replace keyfile.asc by the filename of the trusted key):
  - Windows:
    - From a Command Prompt, Run ```gpg --import keyfile.asc```
  - MacOS:
    - From a Terminal, Run ```gpg --import keyfile.asc```
  - Linux:
    - From a Terminal, Run ```gpg --import keyfile.asc```
- Verify the file signature against the imported (trusted) signature (replace filetoverify.asc by the signature file that was associated with the file, replace filetoverify.txt by the actual file to verify):
  - Windows:
    - Run ```gpg --verify-options show-notations --verify filetoverify.asc filetoverify.txt```
    - Result should show the signature is good and match the trusted signature you imported earlier.
  - MacOS:
    - Run ```gpg --verify-options show-notations --verify filetoverify.asc filetoverify.txt```
    - Result should show the signature is good and match the trusted signature you imported earlier.
  - Linux:
    - Run ```gpg --verify-options show-notations --verify filetoverify.asc filetoverify.txt```
    - Result should show the signature is good and match the trusted signature you imported earlier.

For some other tutorials, please see:

- https://support.torproject.org/tbb/how-to-verify-signature/ [Archive.org]
- https://tails.boum.org/install/vm-download/index.en.html [Archive.org] (See Basic OpenPGP verification).
- https://www.whonix.org/wiki/Verify_the_Whonix_images [Archive.org]

All these guides should also apply to any other file with any other key.

Security (checking for actual malware):

Every check should ideally happen in sandboxed/hardened Virtual Machines. This is to mitigate the possibilities for malware to access your Host computer.

Anti-Virus Software:

You might be asking yourself, what about Anti-Virus solutions? Well, no … these are not perfect solutions against many modern malware and viruses using polymorphic code[447]. But it does not mean they cannot help against less sophisticated and known attacks. It depends how to use them as AV software can become an attack vector in itself.

Again, this is all a matter of threat modeling. Can AV software help you against the NSA? Probably not. Can it help you against less resourceful adversaries using known malware? Probably.

Some will just argue against them broadly like Whonix[448] but this topic is being discussed and disputed even at Whonix[449] by other members of their community.

Contrary to popular myths perpetuating the idea that only Windows is subject to malware and that detection tools are useless on Linux and MacOS:

---

[447] Wikipedia, Polymorphic Code https://en.wikipedia.org/wiki/Polymorphic_code [Wikiless] [Archive.org]

[448] Whonix Documentation, Use of AV, https://www.whonix.org/wiki/Malware_and_Firmware_Trojans#The_Utility_of_Antivirus_Tools [Archive.org]

[449] Whonix Forums, https://forums.whonix.org/t/installation-of-antivirus-scanners-by-default/9755/8 [Archive org]

- Yes, there are viruses and malware for Linux[450, 451, 452, 453, 454]
- Yes, there are viruses and malware for MacOS[450, 455456, 457458]

My personal take on the matter is on the pragmatic side. I think there is still a room for some AV software for some selective and limited use. But it depends which one and how you use them.

- Do not use them AV software with real-time protection as they often run with administration privileges and can become an attack vector.
- Do not use Commercial AV software that uses any "cloud protection", or sends extensive telemetry and samples to their company.
- Do use Open-Source non-real time offline Anti-Virus/Anti-Malware tools as an added measure to scan some files such as:
    - Windows/Linux/MacOS/Qubes OS: ClamAV (https://www.clamav.net/ [Archive.org])
    - Linux/Qubes OS: RFXN Linux Malware Detect (https://github.com/rfxn/linux-malware-detect [Archive org])
    - Linux/Qubes OS: Chkrootkit (http://www.chkrootkit.org/ [Archive.org])
- You could also use online services for **non-sensitive files*** such as VirusTotal (https://www.virustotal.com/gui) or Hybrid-analysis (https://hybrid-analysis.com/).
    - You could also just check the VirusTotal database for the hash of your file if you don't want to send it over (see https://developers.virustotal.com/v3.0/docs/search-by-hash [Archive.org] (See the Integrity (if available): section again for guidance on how to generate hashes).
    - Other tools are also available for non-sensitive files and a convenient list is right here: https://github.com/rshipp/awesome-malware-analysis#online-scanners-and-sandboxes [Archive org]

*** Please be aware that while VirusTotal might seem very practical for scanning various files, their "privacy policy" is problematic (see https://support.virustotal.com/hc/en-us/articles/115002168385-Privacy-Policy [Archive.org]) and states:**

"When you submit Samples to the Services, if you submit Samples to the Services, we will collect all of the information in the Sample itself and information about the act of submitting it".

So, remember that any document you submit to them will be kept, shared, and used commercially including the content. So, you should not do that with sensitive information and rely on various local AV scanners (that do not send samples online).

So, if you are in doubt:

- For non-sensitive files, I do encourage you to check any documents/images/videos/archives/programs you intend to open with VirusTotal (or other similar tools) because … Why not? (Either by uploading or checking hashes).

---

[450] AV-Test Security Report 2018-2019, https://www.av-test.org/fileadmin/pdf/security_report/AV-TEST_Security_Report_2018-2019.pdf [Archive.org]

[451] ZDNet, ESET discovers 21 new Linux malware families https://www.zdnet.com/article/eset-discovers-21-new-linux-malware-families/ [Archive.org]

[452] NakeSecurity, EvilGnome – Linux malware aimed at your desktop, not your servers https://nakedsecurity.sophos.com/2019/07/25/evilgnome-linux-malware-aimed-at-your-laptop-not-your-servers/ [Archive.org]

[453] Immunify, HiddenWasp: How to detect malware hidden on Linux & IoT https://blog.imunify360.com/hiddenwasp-how-to-detect-malware-hidden-on-linux-iot [Archive.org]

[454] Wikipedia, Linux Malware https://en.wikipedia.org/wiki/Linux_malware [Wikiless] [Archive org]

[455] Wikipedia, MacOS Malware https://en.wikipedia.org/wiki/MacOS_malware [Wikiless] [Archive org]

[456] MacWorld, List of Mac viruses, malware and security flaws https://www.macworld.co.uk/feature/mac-viruses-list-3668354/ [Archive org]

[457] JAMF, The Mac Malware of 2020 https://resources.jamf.com/documents/macmalware-2020.pdf [Archive.org]

[458] MacOS Security and Privacy Guide, https://github.com/drduh/macOS-Security-and-Privacy-Guide#viruses-and-malware [Archive org]

- For sensitive files, I would recommend at least an offline unprivileged ClamAV scan of the files.

For instance, this guide's PDF files were submitted to VirusTotal because it is meant to be public knowledge and I see no valid argument against it. It does not guarantee the absence of malware but it does not hurt to add this check.

Manual Reviews:

You can also try to check various files for malware using various tools. This can be done as an extra-measure and is especially useful with documents rather than apps and various executables.

These methods require more tinkering but can be useful if you want to go the extra length.

PDF files:

Again, regarding the PDFs of this guide and as explained in the README of my repository, you could check for anomalies using PDFID which you can download at https://blog.didierstevens.com/programs/pdf-tools/ [Archive.org]

- Install Python 3 (on Windows/Linux/MacOS/Qubes OS)
- Download PDFID and Extract the files
- Run "python pdfid.py file-to-check.pdf" and you should see these at 0 in the case of the PDF files in this repository:

```
/JS                0 #This indicates the presence of Javascript
/JavaScript        0 #This indicates the presence of Javascript
/AA                0 #This indicates the presence of automatic action on opening
/OpenAction        0 #This indicates the presence of automatic action on opening
/AcroForm          0 #This indicates the presence of AcroForm which could contain JavaScript
/JBIG2Decode       0 #This indicates the use of JBIG2 compression which could be used for obfuscating content
/RichMedia         0 #This indicates the presence rich media within the PDF such as Flash
/Launch            0 #This counts the launch actions
/EmbeddedFile      0 #This indicates there are embedded files within the PDF
/XFA               0 #This indicates the presence of XML Forms within the PDF
```

Now what if you think the PDF is still suspicious? Fear not … there are more things you can do to ensure it is not malicious:

- **Qubes OS:** Consider using https://github.com/QubesOS/qubes-app-linux-pdf-converter [Archive.org] which will convert your PDF into a flattened image file. This should theoretically remove any malicious code in it. Note that this will also render the PDF formatting useless (such as links, headings, bookmarks, and references).
- **(Deprecated) Linux/Qubes OS** (or possibly MacOS through Homebrew or Windows through Cygwin): Consider not using https://github.com/firstlookmedia/pdf-redact-tools [Archive.org] which will also turn your PDF into a flattened image file. Again, this should theoretically remove any malicious code in it. Again, this will also render the PDF formatting useless (such as links, headings, bookmarks, and references). **Note that this tool is deprecated and relies on a library called "ImageMagick" which is known for several security issues[459]. You should not use this tool even if it is recommended in some other guides.**
- **Windows/Linux/Qubes/OS/MacOS:** Consider using https://github.com/firstlookmedia/dangerzone [Archive.org] which was inspired by Qubes PDF Converted above and does the same but is well maintained and works on all OSes. This tool also works with Images, ODF files and Office files (Warning: On Windows, this tool requires Docker-Desktop installed and this might (will) interfere with Virtualbox and other Virtualization software because it requires enabling Hyper-V. VirtualBox and Hyper-V do not play nice together[460]. Consider installing this within a Linux VM for convenience instead of a Windows OS).

[459] ImageTragick.com, https://imagetragick.com/ [Archive.org]

[460] Oracle Virtualbox Documentation, https://docs.oracle.com/en/virtualization/virtualbox/6.0/admin/hyperv-support.html [Archive org]

Other type of files:

Here are some various resources for this purpose where you will find what tool to use for what type:

- For Documents/Pictures: Consider using https://github.com/firstlookmedia/dangerzone [Archive.org] which was inspired by Qubes PDF Converted above and does the same but is well maintained and works on all OSes. This tool also works with Images, ODF files and Office files (Warning: On Windows, this tool requires Docker-Desktop installed and this might (will) interfere with Virtualbox and other Virtualization software because it requires enabling Hyper-V. VirtualBox and Hyper-V do not play nice together[461]. Consider installing this within a Linux VM for convenience instead of a Windows OS).
- This practical cheat sheet from SANS: https://digital-forensics.sans.org/media/analyzing-malicious-document-files.pdf [Archive.org] (warning, many of those tools might be harder to use on Windows and you might consider using them from a Linux OS such as Tails, Whonix Workstation or a Linux distribution of your choice as explained later in this guide. There are also other guides out there[462] that might be of use).
- This GitHub repository with various resources on malware analysis: https://github.com/rshipp/awesome-malware-analysis [Archive.org]
- This interesting PDF detailing which tool to use for which file type https://www.winitor.com/pdf/Malware-Analysis-Fundamentals-Files-Tools.pdf [Archive.org]

Even with all those resources, keep in mind you might still get advanced malware if those are not detected by those various tools. Be careful and remember to handle these files within Virtual Machines, if possible, to limit the attack surface and vectors.

Appendix U: How to bypass (some) local restrictions on supervised computers

There might be situations where the only device you have at your disposal is not really yours such as:

- Using a Work computer with restrictions in place on what you can do/run.
- Misuse of Parental control features to monitor your computer usage (despite you being a non-consenting Adult).
- Misuse of various monitoring apps to monitor your computer usage against your will.

The situation might look desperate but it is not necessarily the case as there are some safe ways to bypass these depending on how well your adversaries did their job securing your computer.

Portable Apps:

There are plenty of methods you could use to bypass those restrictions locally. One of them would be to use portable apps[463]. Those apps do not require installation your system and can be run from an USB key or anywhere else.

But this is not a method I would recommend.

This is because those portable apps will not necessarily hide themselves (or be able to hide themselves) from the usage reports and forensic examination. This method is just too risky and will probably arise issues if noticed if you are in such a hostile environment.

Even the most basic controls (supervision or parental) will send out detailed app usage to your adversary.

Bootable Live Systems:

This method is the one I would recommend in those cases.

[461] Oracle Virtualbox Documentation, https://docs.oracle.com/en/virtualization/virtualbox/6.0/admin/hyperv-support.html [Archive org]

[462] Lenny Zeltser, Analyzing Malicious Documents Cheat Sheet https://zeltser.com/analyzing-malicious-documents/ [Archive.org]

[463] Wikipedia, Portable Applications https://en.wikipedia.org/wiki/Portable_application [Wikiless] [Archive org]

It is relatively easy for your adversary to prevent this by setting up firmware BIOS/UEFI (see Bios/UEFI/Firmware Settings of your laptop) controls but usually most adversaries will overlook this possibility which requires more technical knowledge than just relying on Software.

This method could even decrease suspicion and increase your plausible deniability as your adversaries think they have things under control and that everything appears normal in their reports.

This method only depends on one security feature (that they probably did not turn on in most cases): Boot Security.

Boot Security is divided into several types:

- Simple BIOS/UEFI password preventing the change of the boot order. This means you cannot start such a live system in-place of your supervised OS without providing the BIOS/UEFI password.
- Secure Boot. This is a "standard" feature preventing you from starting unsigned systems from your computer. While this feature could be configured to only allow your supervised system, usually by default it will allow running a whole range of signed systems (signed by Microsoft or the Manufacturer for instance).

Secure Boot is relatively easy to bypass as there are plenty of Live Systems that are now Secure Boot compliant (meaning they are signed) and will be allowed by your laptop.

The BIOS/UEFI password on the other hand is much harder to bypass without risks. In that case you are left with two options:

- Guess/Know the password so that you can change the boot order of your laptop without raising suspicions
- Reset the password using various methods to remove the password. **I would not recommend doing this because if your adversaries went the extra length of enabling this security feature, they probably will be suspicious if it was disabled and this might increase suspicion and decrease your plausible deniability considerably.**

Again, this feature is usually overlooked by most unskilled/lazy adversaries and in my experience left disabled.

This is your best chance into bypassing local controls without traces.

The reason is that most of the controls are within your main Operating System software and only monitor what happens within the Operating System. Those measures will not be able to monitor what happened at the Hardware/Firmware level before the Operating System loads.

Precautions:

While you might be able to bypass local restrictions easily using a Live System such as Tails, remember that your network might also be monitored for unusual activities.

Unusual network activities showing up from a computer at the same time your computer is seemingly powered off might raise suspicions.

If you are to resort to this, you should never ever do so from a monitored/known network but only from a safe different network. Ideally a safe public wi-fi (See Find some safe places with decent public Wi-Fi).

Do not use a live system on a Software supervised/monitored device on a known network.

Refer to the Tails route to achieve this. See The Tails route and the Appendix P: Accessing the internet as safely as possible when Tor and VPNs are not an option sections.

Appendix V: What browser to use in your Guest VM/Disposable VM

There are IMHO 5 possibilities of browser to use on your guest/disposable VM:

- Brave (Chromium based)
- Ungoogled-Chromium
- Edge (Chromium based, Windows Only)
- Firefox

- Tor Browser

Here is a comparison table of one fingerprinting test of various browsers with their native settings (**but Javascript enabled for usability, except for Tor Safest mode**).

Disclaimer: these tests while nice are not conclusive of the real fingerprinting resistance. But they can help compare browsers between each other.

Browser	https://coveryourtracks.eff.org/ Fingerprinting Test with real Ad
Safari (Normal)*	Fail (Unique)
Safari (Private Window) *	Fail (Unique)
Edge (Normal)**	Fail (Unique)
Edge (Private Window) **	Fail (Unique)
Firefox (Normal)	Fail (Unique)
Firefox (Private Window)	Fail (Unique)
Chrome (Normal)	Fail (Unique)
Chrome (Private Window)	Fail (Unique)
Ungoogled-Chromium (Normal)	Fail (Unique)
Ungoogled-Chromium (Private Window)	Fail (Unique)
Brave (Normal)	Passed (Randomized)
Brave (Private Window)	Passed (Randomized)
Brave (Tor Window)	Passed (Randomized)
Tor Browser (Normal mode)	Partial
Tor Browser (Safer mode)	Partial
Tor Browser (Safest mode)	Unknown (Result did not load)

- *: MacOS only. **: Windows only.

Brave:

This is my recommended/preferred choice for a Browser within your guest VMs. This is not my recommended choice for a Browser within your Host OS where I strictly recommend Tor Browser.

Why Brave despite the controversies[464]?

- You will encounter less issues later with account creations (captchas …). This is based on my experiences trying to create plenty of online identities using various browsers. You will have to trust me on that.
- You will enjoy native ad-blocking where none is available in others by default without adding extensions.
- Performance is arguably better than Firefox[465].
- Brave is arguably better at fingerprinting resistance than others[466].
- Security of Chromium based Browser is arguably better than Firefox[467,468]. Within the context of this guide, security should be privileged to prevent any vulnerability or exploit from gaining access to the VM.
- Comparison of both by Mozilla: https://www.mozilla.org/en-US/firefox/browsers/compare/brave/ [Archive.org]
- The whole traffic will be routed over a VPN over Tor anyway. So even if you mistakenly opt-in for some telemetry, it is not so important. Remember that in this anonymity threat model, we are mostly after

[464] BlackGNU, https://ebin.city/~werwolf/posts/brave-is-shit/ [Archive.org]
[465] VentureBeat, Browser benchmark battle January 2020: Chrome vs. Firefox vs. Edge vs. Brave https://venturebeat.com/2020/01/15/browser-benchmark-battle-january-2020-chrome-firefox-edge-brave/view-all/ [Archive.org]
[466] Brave.com, Brave, Fingerprinting, and Privacy Budgets https://brave.com/brave-fingerprinting-and-privacy-budgets/ [Archive.org]
[467] Madaidan Insecurities, Firefox and Chromium https://madaidans-insecurities.github.io/firefox-chromium.html [Archive.org]
[468] GrapheneOS, Web Browsing https://grapheneos.org/usage#web-browsing [Archive.org]

anonymity and security. The privacy of our online identities does not matter that much unless the privacy issue is also a security issue that could help deanonymize you.

Ungoogled-Chromium:

Ungoogled-Chromium is a Chromium based Browser with all the Google bits removed (https://github.com/Eloston/ungoogled-chromium [Archive.org]).

It is a solid choice for Privacy and Security concerned individuals. It has many of the benefits of Brave:

- You will encounter less issues later with account creations (captchas …). This is based on my experiences trying to create plenty of online identities using various browsers. You will have to trust me on that.
- Better Security than Firefox as it is Chromium based[469, 470].
- Better Performance than Firefox
- The whole traffic will be router through Tor anyway.

But some cons:

- No Automatic Updates
- No native access to the Extension stores (you will have to install extensions manually)
- No Native Ad-Blocking
- No Native Fingerprinting resistance (you will need extensions for that)

Edge:

This is for Windows users only. Edge is a solid choice too.

- You will encounter less issues later with account creations (captchas …). This is based on my experiences trying to create plenty of online identities using various browsers. You will have to trust me on that.
- Better Security than Firefox as it is Chromium based[471, 472].
- Better Performance than Firefox.
- The whole traffic will be router through Tor anyway.
- Can benefit from additional security using Windows Defender Application Guard (WDAG)[473]. Note that this feature cannot be enabled in a Virtualbox VM unfortunately.
- Native tracker blocking (Similar to Brave Shields).

But some cons:

- You will have to disable some telemetry within the Browser

Firefox:

And of course, lastly you could go with Firefox,

Pros:

- Well, it is out of the "Chromium" world and not participating in expanding Chromium market share
- In addition to being out of the Chromium world, it is also completely out of the Google world (despite the Mozilla Foundation being almost entirely funded by Google[474]).
- Impressive amount of customization through extensions for every possible need.
- Firefox can be severely hardened to almost match the security of Chromium based browsers.

---

[469] Madaidan Insecurities, Firefox and Chromium https://madaidans-insecurities.github.io/firefox-chromium.html [Archive.org]
[470] GrapheneOS, Web Browsing https://grapheneos.org/usage#web-browsing [Archive.org]
[471] Madaidan Insecurities, Firefox and Chromium https://madaidans-insecurities.github.io/firefox-chromium.html [Archive.org]
[472] GrapheneOS, Web Browsing https://grapheneos.org/usage#web-browsing [Archive.org]
[473] Microsoft.com, Microsoft Edge support for Microsoft Defender Application Guard https://docs.microsoft.com/en-us/deployedge/microsoft-edge-security-windows-defender-application-guard [Archive.org]
[474] PcMag, Mozilla Signs Lucrative 3-Year Google Search Deal for Firefox https://www.pcmag.com/news/mozilla-signs-lucrative-3-year-google-search-deal-for-firefox [Archive.org]

Cons:

- Poorer performance compared to Chromium.
- Security (especially sandboxing) of Firefox is arguably weaker than Chromium based browsers[475].
- You will experience more captchas (this is based on my tests).

Tor Browser:

If you are extra paranoid and want to use Tor Browser and have "Tor over VPN over Tor", you could go with Tor Browser within the VM as well. This is IMHO completely pointless/useless.

I would not recommend this option. It is just silly.

Appendix V1: Hardening your Browsers:

Brave:

- Download and install Brave browser from https://brave.com/download/ [Archive org]
- Open Brave Browser
- Go into Settings
- Go to Appearances
  - Disable Show Top Sites
  - Disable Show Brave Suggested Sites
  - Enable Hide Brave Rewards
  - Enable Always show full URL
- Go into Shields
  - Set Shields to Advanced
  - Set Trackers and Ads blocking to Aggressive
  - Set Upgrade to HTTPS to enabled
  - Set Cookie blocking to "Only cross-site"
  - Set Fingerprinting blocking to Standard (or Strict)
- Go into Social media Blocking
  - Uncheck everything unless needed
- Go to Search Engine
  - Pick the one you want (I recommend StartPage or DuckDuckGo)
- Go into Extensions
  - Disable everything except Private Windows with Tor and both Resolve methods set to "Ask"
- Go into Wallet
  - Disable the wallet
- Go into Additional Settings, Privacy and Security
  - Leave WebRTC to Default
  - Disable all the rest
  - Go into Clear Browsing Data
  - Select On Exit
  - Check all options
- Open a new Tab
- Click Customize in the lower right corner
  - Disable everything except maybe the clock
- Navigate to brave://adblock
  - Select any additional adblocking filter you want
- Do not ever enable Brave Rewards (button should be hidden)

[475] Madaidan Insecurities, Firefox and Chromium https://madaidans-insecurities.github.io/firefox-chromium.html [Archive.org]

That's it and you should be pretty much covered. For full paranoia, you can also just "Block Scripts" to disable Javascript.

Ungoogled-Chromium:

Well, upon first run:

- Open Settings
- Open Privacy and Security
  - Open Site Settings
    - Disable All Permissions
- Open Search Engine
  - Select DuckDuckGo
- Navigate to chrome://flags/
  - Search for " fingerprint "
    - Enable " Enable Canvas::measureText() fingerprint deception "
    - Enable " Enable Canvas image data fingerprint deception "
    - Enable " Enable get*ClientRects() fingerprint deception "
  - Search for " WebRTC)
    - Enable " Anonymize local IPs exposed by WebRTC. "
  - Search for " Insecure "
    - Enable " Block insecure private network requests. "

Then, you could install some extensions. If you want to automate this process, you will need to "re-google" some of the Browser by allowing access to Chrome Extension Store. This can be done using this extension: https://github.com/NeverDecaf/chromium-web-store

Otherwise, you will have to do this **manually** as explained below:

- Download first:
  - uBlock Origin: Download the latest zip release from https://github.com/gorhill/uBlock/releases
  - NoScript: Download the latest zip release from https://github.com/hackademix/noscript/releases
  - HTTPS Everywhere: Download the latest zip (for Edge) from https://github.com/EFForg/https-everywhere/releases
  - LocalCDN: Download the latest source zip from https://codeberg.org/nobody/LocalCDN/releases
  - DecentralEyes: Download the latest zip (not the CRX) file from https://github.com/Synzvato/decentraleyes/releases
  - ClearURLs: Download the latest zip (not source code) from https://github.com/ClearURLs/Addon/releases
  - PrivacyBadger: Download the latest zip from https://github.com/EFForg/privacybadger/releases **(warning for this one, unpack and use the src subfolder)**
- Unzip all the files
- Open the Extensions (More Tools > Extensions)
- Switch Developer mode ON
- Click on "Load Unpacked"
- Select the folder of each unzipped file where you see the "manifest.json" file (usually the root one except for PrivacyBager where it is in the /src subfolder)

Now you can configure each extension to your liking. Updates are manual for both Ungoogled-Chromium and each Extension. So, make sure to watch the repositories for new releases.

Edge:

Windows only:

- Open Edge
- Go into Settings

- Go to Profiles and make sure everything is unchecked in every section (Personal Info, Passwords, Payment info, Profile preferences)
- Go to Privacy, search, and services:
    - Go to Tracking Prevention:
        - Set to Strict or at least Balanced
        - Set to always use Strict with InPrivate Windows
    - Go to Privacy:
        - Enable send Do Not Track
        - Disable the options for website to check your payment methods
    - Go to Optional Diagnostic Data:
        - Disable it
    - Go to Personalize your Web Experience:
        - Disable it
    - Go to Security
        - Disable everything
    - Go to Services
        - Disable everything
        - In Address Bar and Search:
            - Disable everything and change the search engine to DuckDuckGo
    - Go to Cookies and Sites Permissions:
        - Within All Permissions:
            - Within Cookies, make sure "Block Third Party Cookies" is checked
            - Block everything except:
                - Javascript
                - Images

Enable Application Guard for Edge (only on Host OS, not possible within a VirtualBox VM):

Skip if this is a VM

- Open Control Panel.
- Click on Programs
- Click on Turn Windows features on or off link
- Check the Windows Defender Application Guard option
- Click OK.
- Click Restart.
- Now you can open Edge and open a new "Application Guard" Window.

That's about it for Edge but you are also free to add extensions from the Chrome Store such as:

- uBlock
- LocalCDN or DecentralEyes
- PrivacyBadger
- HTTPSEverywhere
- NoScript
- ClearURLs

Firefox:

Normal settings:

- Open Firefox
- On the Firefox Home Page:
    - Click Personalize
    - Uncheck/Disable Everything
- Open Settings:

- Go into Search
  - Change the search engine to DuckDuckGo
- Go into Privacy & Security
  - Set to Custom
    - Cookies: Select All Third-Party Cookies
    - Tracking Content: In all Windows
    - Check Cryptominers
    - Check Fingerprinters
  - Set always send "Do Not Track"
- Go to Logins and Passwords
  - Uncheck "ask to save logins and passwords for websites"
- Go to Permissions
  - Location: check block new requests
  - Camera: check block new requests
  - Microphone: check block new requests
  - Notifications: check block new requests
  - Autoplay: select Disable Audio and Video
  - Virtual Reality: check block new requests
  - Check Block Pop-ups
  - Check Warn when websites try to install add-ons
- Go to Firefox Data Collection and Use
  - Disable everything
- Go to HTTPS-Only Mode
  - Enable it on all Windows

Advanced settings:

- Navigate to about:config
- Click Accept the Risk and Continue
  - Safe Settings (should not break anything)
    - Disable Firefox Pocket
      - Set "extensions.pocket.enabled" to false
    - Disable All Telemetry
      - Set " browser.newtabpage.activity-stream.feeds.telemetry " to false
      - Set " browser.ping-centre.telemetry " to false
      - Set " browser.tabs.crashReporting.sendReport " to false
      - Set " devtools.onboarding.telemetry.logged " to false
      - Set " toolkit.telemetry.enabled " to false
      - Search for " toolkit.telemetry.server " and clear it
      - Set " toolkit.telemetry.unified " to false
    - Disable Pre-Fetching
      - Set " network.dns.disablePrefetch " to true
      - Set " network.prefetch-next " to false
    - Disable Javascript in PDFs
      - Set " pdfjs.enableScripting " to false
    - Disable obsolete SSL encryption
      - Set " security.ssl3.rsa_des_ede3_sha " to false
      - Set " security.ssl.require_safe_negotiation " to true
    - Disable Firefox Accounts
      - Set " identity.fxaccounts.enabled " to false
    - Disable Geolocation
      - Set " geo.enabled " to false
    - Disable Web Notifications

        - Set " dom.webnotifications.enabled " to false
    - Moderate Settings (could break some websites)
        - Disable WebRTC (this will break all websites with video/audio communications)
            - Set " media.peerconnection.enabled " to false
            - Set " media.navigator.enabled " to false
        - Disable WebGL (this will break some media intensive websites)
            - Set " webgl.disabled " to true
    - Advanced (this will break some websites)
        - Set " privacy.resistFingerprinting " to true
        - Set " network.http.sendRefererHeader " to 0 (this might break plenty of websites)
        - Set " change privacy.firstparty.isolate " to true
        - Set " change network.cookie.lifetimePolicy " to 2 (this deletes all cookies after each session)
        - Set " network.http.referer.XOriginPolicy " to 2 (Send Referer only when the full hostnames match)

Addons to install/consider:

- uBlock Origin (https://addons.mozilla.org/en-US/firefox/addon/ublock-origin/)
- LocalCDN (https://addons.mozilla.org/en-US/firefox/addon/localcdn-fork-of-decentraleyes/) or Decentraleyes (https://addons.mozilla.org/en-US/firefox/addon/decentraleyes/)
- HTTPS Everywhere (https://addons.mozilla.org/en-US/firefox/addon/https-everywhere/)
- NoScript (https://addons.mozilla.org/en-US/firefox/addon/noscript/)
    - Within the options, Change Default options to check everything except "Ping" and "Unrestricted CSS"
- ClearURLs (https://addons.mozilla.org/en-US/firefox/addon/clearurls/)
- PrivacyBadger (https://addons.mozilla.org/en-US/firefox/addon/privacy-badger17/)
- Temporary Containers (https://addons.mozilla.org/en-US/firefox/addon/temporary-containers/)
- Privacy Settings (https://addons.mozilla.org/en-US/firefox/addon/privacy-settings/)

Bonus resources:

Here are also two recent guides to harden Firefox:

- https://chrisx.xyz/blog/yet-another-firefox-hardening-guide/ [Archive.org]
- https://ebin.city/~werwolf/posts/firefox-hardening-guide/ [Archive.org]

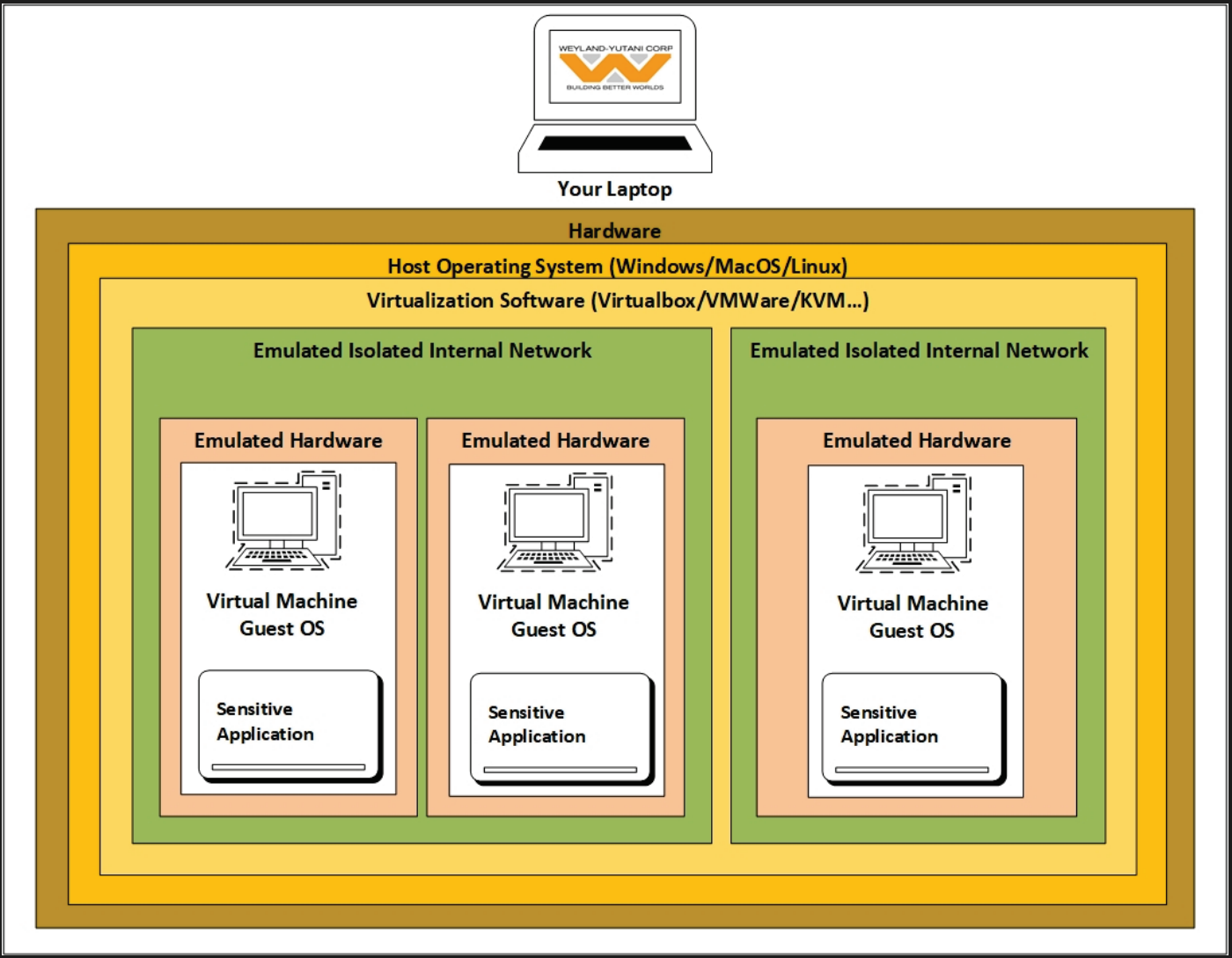
Appendix W: Virtualization

So, you might ask yourself, what is Virtualization[476]?

Basically, it is like the Inception movie with computers. You have emulated software computers called Virtual Machines running on a physical computer. And you can even have Virtual Machines running within Virtual machines if you want to (but this will require a more powerful laptop in some cases).

Here is a little basic illustration of what Virtualization is:

[476] Wikipedia, Virtualization https://en.wikipedia.org/wiki/Virtualization [Wikiless] [Archive.org]



Each Virtual Machine is a sandbox. Remember the reasons for using them is to prevent the following risks:

- Mitigate local data leaks and ease clean-up in case of risk (everything is contained within the VM and only the VM identifiers could be leaked and not the Host Hardware identifiers)
- Reduce malware/exploit attack surfaces (if your VM is compromised, the adversary still must figure out he is in a VM and then gain access to the Host OS which is not so trivial).
- Mitigate online data leaks by being able to enforce strict network rules on Virtual Machines for accessing the network (such as passing through the Tor Network).

Appendix X: Using Tor bridges in hostile environments

In some environments, your ISPs might be trying to prevent you from accessing Tor. Or accessing Tor openly might be a safety risk.

In those cases, it might be necessary to use Tor bridges to connect to the Tor network (see Tor Documentation https://2019.www.torproject.org/docs/bridges [Archive.org] and Whonix Documentation https://www.whonix.org/wiki/Bridges [Archive org]).

Bridges are special Tor entry nodes that are not listed on the Tor public directory. Some of those are running on people running the Snowflake Browser extension[477] while others are running on various servers around the world. Most of those bridges are running some type of obfuscation method called obfs4[478].

[477] Tor Project, Project Snowflake https://snowflake.torproject.org/ [Archive.org]

[478] GitHub, Obfs4 Repository https://github.com/Yawning/obfs4/ [Archive org]

Here is the definition from the Tor Browser Manual[479]: "obfs4 makes Tor traffic look random, and prevents censors from finding bridges by Internet scanning. obfs4 bridges are less likely to be blocked than its predecessor, obfs3 bridges".

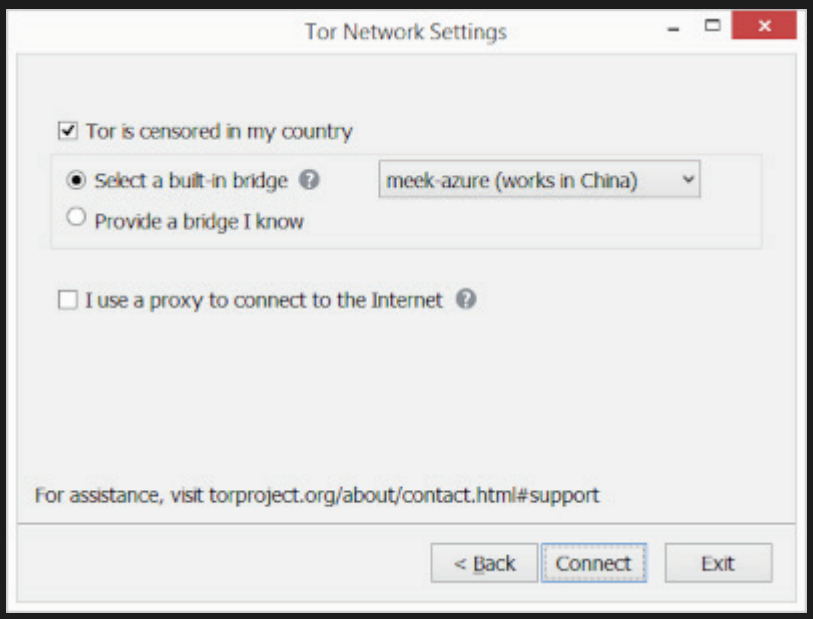
Some of those are called "Meek" bridges and are using a technique called "Domain Fronting" where your Tor client (Tails, Tor Browser, Whonix Gateway) will connect to a common CDN used by other services. To a censor, it would appear you are connecting to a normal website such as Microsoft.com. See https://gitlab.torproject.org/legacy/trac/-/wikis/doc/meek for more information.

As per their definition from their manual[480]: "meek transports make it look like you are browsing a major web site instead of using Tor. meek-azure makes it look like you are using a Microsoft web site".

Lastly, there are also bridges called Snowflake bridges that rely on users running the snowflake extension in their browser to become themselves entry nodes. See https://snowflake.torproject.org/ [Archive.org].

First you should, proceed with the following checklist to make sure you cannot circumvent Tor Blocking (double-check) and try to use Tor Bridges (https://bridges.torproject.org/ [Archive.org]).

- (Recommended if blocked but **safe**) Try to get an obfs4 bridge in the Tor connection options.
- (Recommended if blocked but **safe**) Try to get a snowflake bridge in the Tor connection options.
- **(Recommended if hostile/risky environment)** Try to get a meek bridge in the Tor connection options (might be your only option if you are for instance in China).



If none of those build-in methods are working, you could try getting a manual bridge either from:

- https://bridges.torproject.org/bridges?transport=meek (for a meek bridge)
- https://bridges.torproject.org/bridges?transport=obfs4 (for an obfs4 bridge)

This website obviously could be blocked/monitored too so you could instead (if you have the ability) ask someone to do this for you if you have a trusted contact and some e2e encrypted messaging app.

Finally, you could also request a bridge request by e-mail to bridges@torproject.org with the subject empty and the body being: "get transport obfs4" or "get transport meek". There is some limitation with this method tho as it is only available from a Gmail e-mail address or a Riseup.net (https://riseup.net/) e-mail address.

Hopefully these bridges should be enough to get you connected even in a hostile environment.

If not, consider Appendix P: Accessing the internet as safely as possible when Tor and VPNs are not an option

[479] Tor Browser Manual, Pluggable Transport https://tb-manual.torproject.org/circumvention/ [Archive.org]

[480] Tor Browser Manual, Pluggable Transport https://tb-manual.torproject.org/circumvention/ [Archive.org]

Appendix Y: Windows AME download and installation

This is the Windows 10 AME installation process that should be valid for any Windows 10 AME install within this guide.

Important notes:

- **Windows 10 AME itself cannot be updated including security updates. You must use their latest release as is provided by them or build it yourself following their project instructions.**
- **Apps however can be installed/updated without issues.**
- **This version has no anti-virus at all and so you should be extra-careful when running things.**
- **This project is more known than you think: https://www.youtube.com/watch?v=nwkiU6GG-YU** [Invidious]
- **I checked myself the latest release (AME_20H2_(2021-04-01).iso) for viruses/malware using various AVs and it came out clean. I cannot vouch for any further releases.**
- **Yes, if you want to use this as your Host OS, you can do so too.**

Download:

Unfortunately, this build of Windows can only be downloaded through a Torrent client by fetching the torrent file on their Telegram group @amereleases. Use Telegram desktop for this. This does require a valid Telegram account with a registered phone number which is a bad point.

Here is a magnet link to their latest release (AME_20H2_(2021-04-01).iso) **as of the writing of this guide** (this might be outdated and you should check their website if a new one is available, you can preview this without telegram by going to https://t.me/s/amereleases) so you can skip the Telegram channel (open this link with any Torrent client, personally I recommend qBittorrent https://www.qbittorrent.org/):

Within qBittorrent, just open the following magnet link (without quotes):

```magnet:?xt=urn:btih:a21e7dba7f0615ae3377dfaca3dddac9c5cf2e86&dn=AME_20H2_(2021-04-01).iso&tr=http%3a%2f%2ftracker2.wasabii.com.tw%3a6969%2fannounce&tr=udp%3a%2f%2ftracker.sktorrent.net%3a6969%2fannounce&tr=http%3a%2f%2fwww.wareztorrent.com%3a80%2fannounce&tr=udp%3a%2f%2fbt.xxx-tracker.com%3a2710%2fannounce&tr=udp%3a%2f%2ftracker.eddie4.nl%3a6969%2fannounce&tr=udp%3a%2f%2ftracker.grepler.com%3a6969%2fannounce&tr=udp%3a%2f%2ftracker.mg64.net%3a2710%2fannounce&tr=udp%3a%2f%2fwambo.club%3a1337%2fannounce&tr=udp%3a%2f%2ftracker.dutchtracking.com%3a6969%2fannounce&tr=udp%3a%2f%2ftc.animereactor.ru%3a8082%2fannounce&tr=udp%3a%2f%2ftracker.justseed.it%3a1337%2fannounce&tr=udp%3a%2f%2ftracker.leechers-paradise.org%3a6969%2fannounce&tr=udp%3a%2f%2ftracker.opentrackr.org%3a1337%2fannounce&tr=https%3a%2f%2fopen.kickasstracker.com%3a443%2fannounce&tr=udp%3a%2f%2ftracker.coppersurfer.tk%3a6969%2fannounce&tr=udp%3a%2f%2fopen.stealth.si%3a80%2fannounce&tr=http%3a%2f%2f87.253.152.137%2fannounce&tr=http%3a%2f%2f91.216.110.47%2fannounce&tr=http%3a%2f%2f91.217.91.21%3a3218%2fannounce&tr=http%3a%2f%2f91.218.230.81%3a6969%2fannounce&tr=http%3a%2f%2f93.92.64.5%2fannounce&tr=http%3a%2f%2fatrack.pow7.com%2fannounce&tr=http%3a%2f%2fbt.henbt.com%3a2710%2fannounce&tr=http%3a%2f%2fbt.pusacg.org%3a8080%2fannounce&tr=https%3a%2f%2ftracker.bt-hash.com%3a443%2fannounce&tr=udp%3a%2f%2ftracker.leechers-paradise.org%3a6969&tr=https%3a%2f%2f182.176.139.129%3a6969%2fannounce&tr=udp%3a%2f%2fzephir.monoculus.us%3a6969%2fannounce&tr=https%3a%2f%2ftracker.dutchtracking.com%3a80%2fannounce&tr=https%3a%2f%2fgrifon.info%3a80%2fannounce&tr=udp%3a%2f%2ftracker.kicks-ass.net%3a80%2fannounce&tr=udp%3a%2f%2fp4p.arenabg.com%3a1337%2fannounce&tr=udp%3a%2f%2ftracker.aletorrenty.pl%3a2710%2fannounce&tr=udp%3a%2f%2ftracker.internetwarriors.net%3a1337%2fannounce&tr=https%3a%2f%2ftracker.parrotsec.org%3a443%2fannounce&tr=https%3a%2f%2ftracker.moxing.party%3a6969%2fannounce&tr=https%3a%2f%2ftracker.ipv6tracker.ru%3a80%2fannounce&tr=https%3a%2f%2ftracker.fastdownload.xyz%3a443%2fannounce&tr=https%3a%2f%2fgwp2-v19.rinet.ru%3a80%2fannounce&tr=https%3a%2f%2ftr.kxmp.cf%3a80%2fannounce&tr=https%3a%2f%2fexplodie.org%3a6969%2fannounce```

Do not forget to remove the torrent and quit qBittorrent when you are done (without deleting the downloaded files).
```

Installation:

The official guide is here: https://telegra.ph/AME-Download-Guide-09-07 [Archive.org]

You can also build this ISO yourself from their scripts if you do not trust their provided ISO release using the guide here: https://wiki.ameliorated.info/doku.php?id=documentation_20H2 [Archive.org]

Here is my guide using their provided ISO file:

- Start the bootable Windows AME install
- Leave language by default (English – United States)
- Select your Keyboard Layout to your keyboard
- Click "Next"
- Select "I don't have a product key"
- Select Custom
- Storage:
    - If this is a simple OS installation (Host OS with Simple Encryption) or VM without encryption, **select the whole disk** and proceed with installation (skip next step).
    - If this is part of a plausible deniability encryption setup on the Host OS:
        - If you are installing Windows for the first time (Hidden OS):
            - Delete the current partitions
            - Create a First partition with at least 50GB of disk space (about a third of the total disk space).
            - Create a Second partition with the remaining two thirds of the total disk space.
        - If you are installing Windows for the second time (Decoy OS):
            - Do not Delete the current partitions
            - Install Windows on the first partition you created during the first install.
        - Proceed with the install in the First partition
- You are done! No privacy settings to set.
- Login with username "user" and password "malte" (check the lower right language and switch to your layout if you do not use a default US English keyboard).

Appendix Z: Paying anonymously online with BTC

There are many services that you might want to use (VPS hosting, mail hosting, domain names…) but require payment of some kind.

As mentioned before in this guide multiple times, I strongly recommend the use of services accepting cash (that you could send anonymously through the postal services) or Monero which you can buy and use directly and safely.

But what if the service you want does not accept Monero but does accept a more mainstream cryptocurrency such as Bitcoin (BTC).

Bitcoin in itself is not anonymous at all (Remember Your Crypto currencies transactions) and you should never ever purchase Bitcoin from an exchange and then use these directly for purchasing services anonymously. This will not work and you can be traced easily.

But it is however possible to anonymize Bitcoin through the use of Monero (XMR) safely using a few more and at a relatively small cost. So, you might be wondering how? Well, it is actually pretty simple:

1. Purchase Monero from the exchange of your choice (this can be Kraken for example or LocalMonero) using your real identity and financial information.
2. Create a Monero wallet on one of your anonymized VMs as explained in this guide before (for example, on the Whonix Workstation which includes a Monero client natively)
3. Transfer your Monero from the Exchange you bought it from to the wallet on your VM.
4. On the same VM (for instance again the Whonix Workstation), create a Bitcoin Wallet (again this is provided natively within the Whonix Workstation)

5. From an anonymized browser (such as Tor Browser), use a non-KYC (Know Your Customer) service swapping service such as Changelly and convert your Monero to BTC and transfer those to the BTC Wallet you have on your anonymized VM

You should now have an anonymized Bitcoin wallet that can be used for purchasing services that do not accept Monero. **You should never ever access this wallet from a non-anonymized environment and always use well-thought opsec with your BTC transactions. Remember those can be traced back to you.**

The origin of those BTC cannot be traced back to your real identity due to the use of Monero.

Bonus step for improving your BTC privacy using obfuscation:

- You might want to consider the use of Wasabi (https://wasabiwallet.io/ [Archive.org]) for your BTC transactions using their "CoinJoin feature"[481] to further cover your tracks. This would mean swapping your Monero for BTC to a Wasabi Wallet instead of a normal Wallet. And then using that Wasabi Wallet for your BTC transactions using their CoinJoin feature.

If you want to get your money back, you will have to do the procedure in reverse. Use a non-KYC swapping service such as Changelly to switch back to Monero and transfer to your Monero wallet. And transfer back those Monero coins to your KYC Exchange (Kraken for instance) where you will be able to sell them again.

Please do read the Monero Disclaimer.

Appendix A1: Recommended VPS hosting providers

I will only recommend providers that accepts Monero as payment and here is my short list:

- **Njalla https://njal.la/ [Archive.org] (my personal favorite, recommended by Privacytools.Io (https://privacytools.io/providers/hosting/ [Archive.org]).**
- **1984.is https://www.1984.is [Archive.org].**

Also consider these lists:

- Tor Project: https://community.torproject.org/relay/community-resources/good-bad-isps/ [Archive org]
- Privacytools.io: https://privacytools.io/providers/hosting/ [Archive org]

Lastly, you could pick one from the list here that does accept Monero:
https://www.getmonero.org/community/merchants/#hosting [Archive.org]

Pease do read the Monero Disclaimer.

If the service does not accept Monero but does accept BTC, consider the following appendix: Appendix Z: Paying anonymously online with BTC.

Appendix A2: Guidelines for passwords and passphrases

My opinion (and the one of many[482, 483, 484, 485, 486, 487]) is that passphrases are generally better than passwords. So instead of thinking of better passwords, forget them altogether and use passphrases instead (when possible). Or just

---

[481] Europol Wasabi Wallet Report, https://www.tbstat.com/wp/uploads/2020/06/Europol-Wasabi-Wallet-Report.pdf [Archive.org]

[482] NIST, https://www.sans.org/blog/nist-has-spoken-death-to-complexity-long-live-the-passphrase/ [Archive.org]

[483] ZDnet, FBI recommends passphrases over password complexity https://www.zdnet.com/article/fbi-recommends-passphrases-over-password-complexity/ [Archive.org]

[484] The Intercept, Passphrases That You Can Memorize — But That Even the NSA Can't Guess
https://theintercept.com/2015/03/26/passphrases-can-memorize-attackers-cant-guess/ [Archive org]

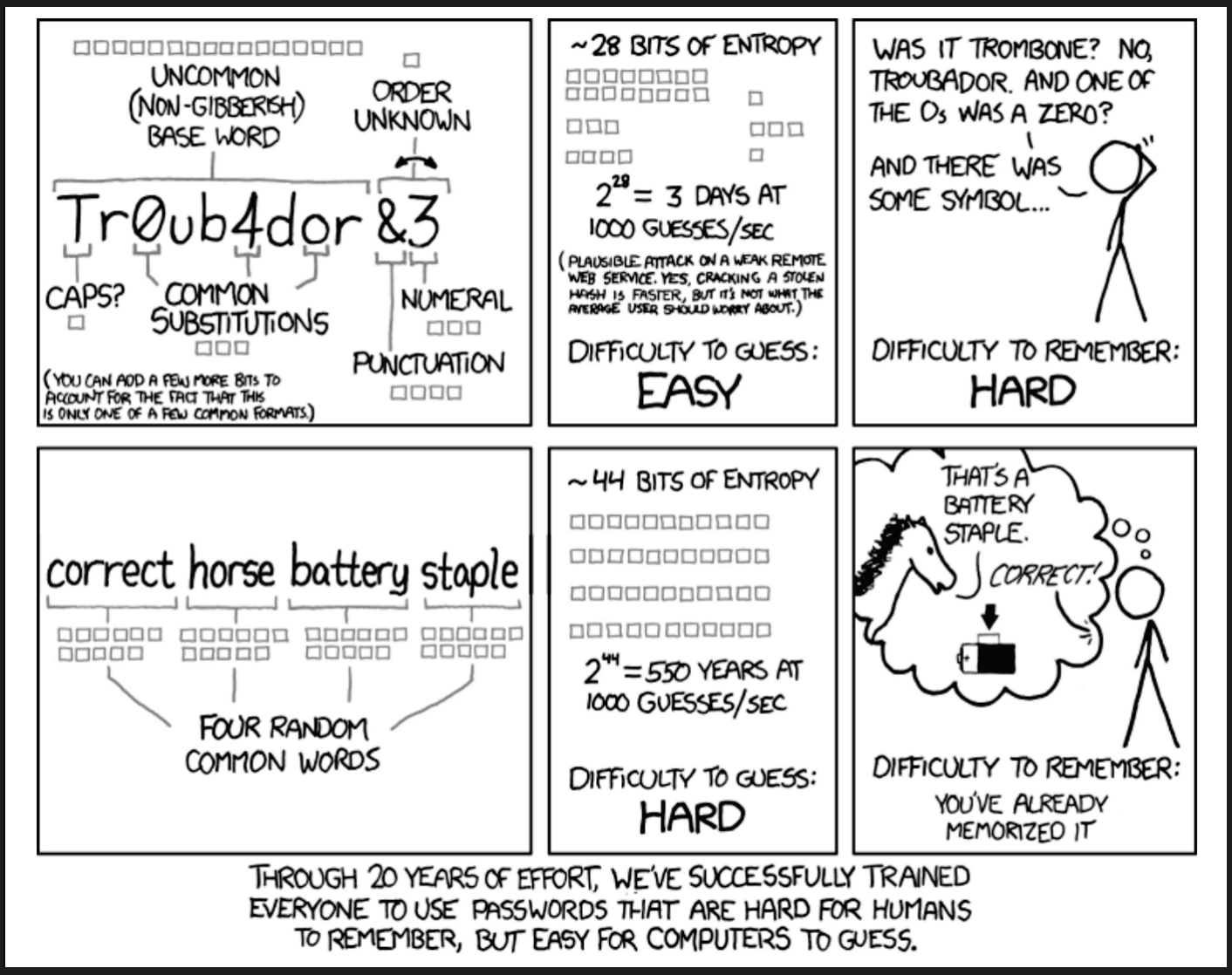
[485] ProtonMail Blog, Let's settle the password vs. passphrase debate once and for all https://protonmail.com/blog/protonmail-com-blog-password-vs-passphrase/ [Archive.org]

[486] YouTube, Edward Snowden on Passwords: Last Week Tonight with John Oliver (HBO)
https://www.youtube.com/watch?v=yzGzB-yYKcc [Invidious]

[487] YouTube, How to Choose a Password – Computerphile https://www.youtube.com/watch?v=3NjQ9b3pgIg [Invidious]

use a password manager with very long passwords (such as KeePassXC, the preferred password manager in this guide).

The well-known shown-below XKCD https://xkcd.com/936/ [Archive.org] is still valid despite some people disputing it (See https://www.explainxkcd.com/wiki/index.php/936:_Password_Strength [Archive.org]). Yes, it is quite old now and is a little bit outdated and might be misinterpreted. But generally speaking, it is still valid and a good argument for using passphrases instead of passwords.



(Illustration by xkcd.com, licensed under CC BY-NC 2.5)

Here are some recommendations (based on Wikipedia[488]):

- Long enough to be hard to guess (typically 4 words is a minimum, 5 or more is better).
- Not a famous quotation from literature, holy books, et cetera.
- Hard to guess by intuition—even by someone who knows the user well.
- Easy to remember and type accurately.
- For better security, any easily memorable encoding at the user's own level can be applied.
- Not reused between sites, applications, and other different sources.
- Do not use only "common words" (like "horse" or "correct")

Watch this insightful video by Computerphile: https://www.youtube.com/watch?v=3NjQ9b3pgIg [Invidious]

[488] Wikipedia, Passphrase https://en.wikipedia.org/wiki/Passphrase#Passphrase_selection [Wikiless] [Archive.org]

Use a different one for each service/device if possible. Do not make it easy for an adversary to access all your information because you used the same passphrase everywhere.

Monero Disclaimer

The anonymity of Monero depends on its crypto algorithms. If you do use Monero from a KYC Exchange. You can be almost certain that you are safe today. But you might not be in the long-term future if Monero algorithms are ever broken[489] (think Quantum Computing). Do keep in mind that KYC regulations might force operators (such as Crypto Exchanges) to keep your financial records for up to 10 years and that you therefore need Monero algorithms to not be broken for the next 10 years as well. **Use at your own risk, sending cash payments to providers accepting cash (through the postal service) is always a better solution if/when possible.**

You may want to watch this insightful video for more details: **https://www.youtube.com/watch?v=j02QoI4ZlnU** [Invidious]

Also please consider reading: **https://github.com/monero-project/monero/blob/master/docs/ANONYMITY_NETWORKS.md#privacy-limitations** [Archive org]

[489] Monero Research Lab, Evaluating cryptocurrency security and privacy in a post-quantum world https://github.com/insight-decentralized-consensus-lab/post-quantum-monero/blob/master/writeups/technical_note.pdf [Archive.org]