The Hitchhiker's Guide to Online Anonymity

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

Version 0.1.10 (draft), December 2020 (work in progress, some parts are incomplete) by AnonymousPlanet.

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

Feel free to discuss ideas using GitHub Discussions at: https://github.com/AnonymousPlanet/thgtoa/discussions

PDF version of this guide at: https://github.com/AnonymousPlanet/thgtoa/raw/main/guide.pdf

Introduction:

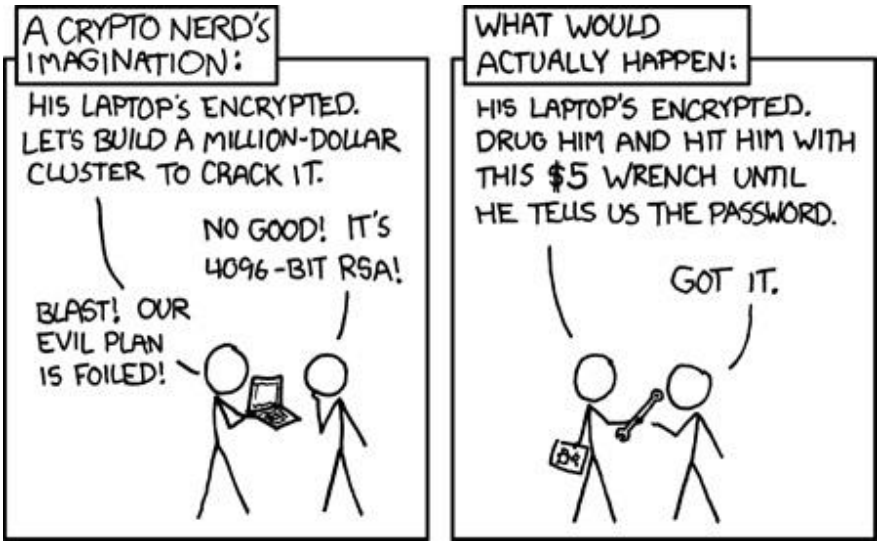
Making a social media account with a pseudonym or artist/brand name is easy. And it's enough is most use cases to protect your identity as the next George Orwell. There are plenty of people using pseudonyms all over Facebook/Instagram/Twitter/LinkedIn/TikTok/Snapchat/Reddit/… But the vast majority of those are anything but anonymous and can easily be traced to their real identity by your local cops, random people within the OSINT[1] (Open-Source Intelligence) community and trolls[2] on 4chan[3].

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 tracking techniques, id verification techniques and guidance to creating and maintaining anonymous identities online including social media accounts safely.

Will this guide help you protect yourself from the NSA, the FSB, Mark Zuckerberg or the Mossad if they're out to find you? Probably not … Mossad will be doing "Mossad things" [4] and will probably find you no matter how hard to try to hide[5].

You have to consider your threat model[6] 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 Belingcat[7] , Doxing[8] trolls on 4chan[9] and others that have no access to the NSA toolbox? More likely. Tho I wouldn't be so sure about 4chan.

It's also important 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. Most of those guidelines are guessed based on experience or based on referenced studies and recommendations by other experts. These experiences take a lot of time and resources and are sometimes far from being scientific. **Your mileage may vary (a lot).**

You might think this guide has no legitimate use but there are many[10,11] such as:

- Evading Censorship
- Evading Oppression
- Evading Unlawful Government Surveillance
- Whistle Blowing
- Journalism
- Activism

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

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 individuals conduct unlawful or unethical activities (such as trolling).
- Use by minors.

If you go through with this long read including the many references, I believe you'll understand most of the current online privacy and anonymity issues.

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

Use at your own risk. Anything in here is not legal advice and you should verify compliance with your local law before use (IANAL[12]).

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[13]). Alternatively be resident of any other country where you can validate and verify this is legal yourself.**
- This guide will assume you already have access to some PC (Windows/Linux) laptop computer (not a work/shared device).
- Don't be evil (for real this time)[14].
- Have patience as this process could take several weeks to finalize.
- Have a little budget to dedicate to this process (you'll need at least budget for an USB key).
- Have a lot of free time on your hands to dedicate to this process.
- Be prepared to read a lot of references (do read them), guides (don't skip them) and follow a lot of how-to tutorials thoroughly (don't skip them either).

This guide will (for the moment) not recommend using MacOS due to the latest Big Sur update which forces "unblockable" telemetry[15,16] and because MacOS doesn't offer MAC address randomization.

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

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.

Here is a non-exhaustive list of some of the many ways you could be de-anonymized:

Your IP address:

Your IP address[17] is the most known and obvious way you can be tracked. That IP is the IP you're 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[18] which 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 won't 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 but also those you used to sign-in.

For those reasons, we'll need to not use 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 WIFI service (free).
- Using an anonymous VPN service[19] (paid by cash).
- Using the Tor Anonymity Network[20] (free).

All those will be explained later in this guide.

Your DNS requests:

DNS stands for "Domain Name System"[21] and is a service used by your browser (and other apps) to find the IP addresses of a service. It's 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 https://www.google.com. Your Browser (Chrome or Firefox) will query a DNS service to find the IP addresses of the Google web servers.

Usually the DNS service is provided by your ISP and automatically configured by the network you're connecting to. This DNS service could also be subject to data retention regulations or will just keep logs for other reasons (data 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[22]. The provided DNS servers will give you a different address (than their real one) for some websites (like redirecting thepiratebay to some govt website). Such blocking is widely applied worldwide for certain sites[23].

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's not encrypted, your ISP and/or any other adversary could still intercept (using a Man-in-the-middle attack[49]) 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're 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[24]. For these devices, you'll have to force them[25] to stop using their hardcoded DNS service which could make them stop working properly.

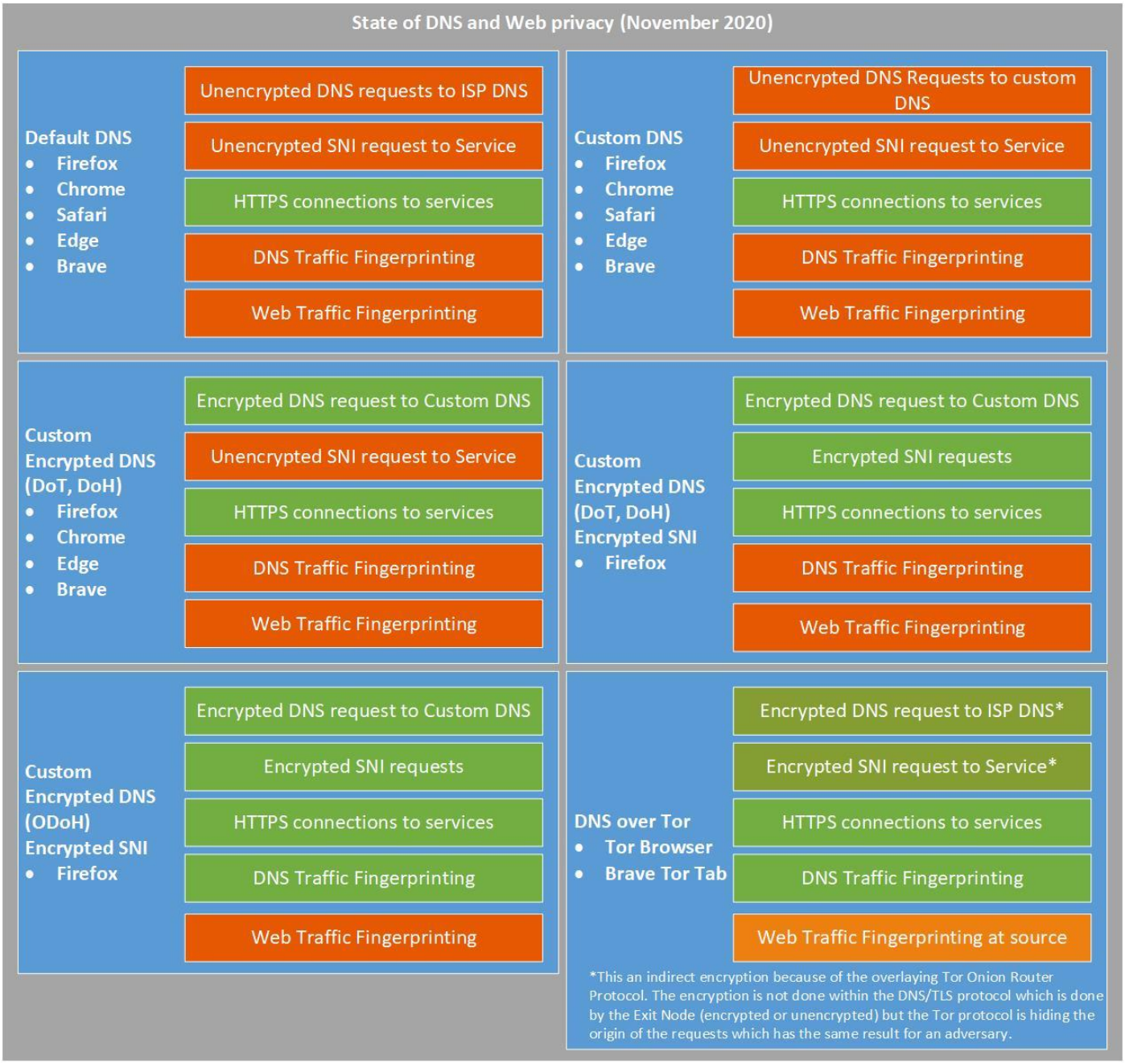
A solution to this is to use encrypted DNS using DNS over HTTPS[26] or DNS over TLS[27] with a private DNS server (this can be self-hosted locally with a solution like pi-hole[28], remotely hosted with a solution like nextdns.io or using the solutions provider by your VPN provider or the Tor network). This should prevent your ISP or some middle-man from snooping on your requests … except it might not.

Unfortunately the TLS protocol used in most HTTPS connections in most Browsers (Chrome/Brave among them) will leak the DNS again through SNI[29] handshakes (this can be checked here at Cloudflare: https://www.cloudflare.com/ssl/encrypted-sni/). Only Firefox as of the writing of this guide supports eSNI (encrypted SNI[30] also called ECH) which will encrypt everything end to end (in addition to using a secure private DNS over TLS/HTTPS) and will allow you to really hide your DNS requests from a third party. Some countries like Russia[31] and China[32] will block eSNI handshakes at network level to allow snooping and prevent bypassing censorship. Meaning you won't be able to establish an HTTPS connection with a service if you don't allow them to see what it was.

Finally, even if you use a custom encrypted DNS server (DoS or DoT) with eSNI support, it might still not be enough as traffic analysis studies[33] have shown it's still possible to reliably fingerprint and block unwanted requests. Only DNS over Tor was able to demonstrate efficient DNS Privacy in recent studies.

One could also decide to use a Tor Hidden DNS Service or Oblivious DNS over HTTPS (ODoH)[34] to further increase privacy/anonymity but unfortunately such services are rare and the only reliable one I know provided by Cloudflare (https://blog.cloudflare.com/welcome-hidden-resolver/, https://blog.cloudflare.com/oblivious-dns/). I **personally** think these are viable technical options but are also a moral choice if you want to use them (despite the risk posed by some researchers[35]).

Here is an illustration showing the current state of DNS privacy:



Therefore to mitigate all this issue (as much as possible), this guide we will later recommend a virtualized multi-layered solution of VPN over Tor (or even Tor over VPN over Tor).

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

The IMEI (International Mobile Equipment Identity[36]) and the IMSI (International Mobile Subscriber Identity[37]) are unique numbers created by mobile phone manufacturers and mobile phone operators.

The IMEI is tied directly to the phone you're 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's not even needed). It's also used by many applications (Banking apps abusing the phone permission on Android for instance[38]) and smartphone Operating Systems (Android/IOS) for identification of the device[39]. It is possible but difficult (and not illegal in many jurisdiction[40]) to change the IMEI on a phone but it's 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're 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 in 2020, 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 5 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 "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[41],[42].
- 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're 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 don't find you on CCTV[43] 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[44].
- Govt agencies around the world interested in your phone number can and do use[45] special devices called "IMSI catchers"[46] like the Stingray[47] or the Nyxcell[48]. These devices are able to impersonate (to spoof) a cell phone Antenna and force a specific IMSI (from your phone) to connect to it to access the cell network. Once they do, they will be able to use various MITM[49] (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: DEF CON Safe Mode - Cooper Quintin - Detecting Fake 4G Base Stations in Real Time https://www.youtube.com/watch?v=siCk4pGGcqA

For these reasons, it's crucial to get a dedicated burner phone with an IMEI that is not tied to you in any way (past or present). As well as it's crucial to get an IMSI (sim card) that is not tied to you in any way. Both need to be bought in a safe place (ideally without CCTV), with cash and without bringing your real phone along. And last but not least due to the third reason mentioned above, 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's not really as these phones are only being used during the setup/sign-up process and for verification from time to time.

For additional safety (if you absolutely have to take your smartphone along with you or if you want to store your Burner phone), you could consider the use of a faraday cage[50] bag to store your devices. There are many such faraday "signal blocking" bags available for sale and some of these have been studied[51] for their effectiveness. If you can't 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).

Your Wi-Fi MAC address:

The MAC address[52] is a unique identifier tied to your physical Network Interface (Wired Ethernet or WIFI) and could of course be used to track you if it's 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's 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 anonymous 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/WIFI access points keeps logs of devices that registered on the Wi-Fi and these can be accessed too to find out who's been using your WIFI. 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).

So it's important again not to bring your phone along when/where you conduct sensitive activities. If you use your own laptop, then it's 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 doesn't support this feature even in its latest Big Sur version.

Your Bluetooth MAC address:

Your Bluetooth MAC is like a MAC address except it's 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[53].

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

Your Operating Systems and Apps telemetry services:

Whether it's Android, IOS, Windows, MacOS or even Ubuntu. Most popular Operating Systems now collect telemetry information by default. This information collection can be extensive and include a staggering amount 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
- IOS/Apple:
  - More information at https://www.apple.com/legal/privacy/en-ww/ and https://support.apple.com/en-us/HT202100
  - Apple does claim[54] that they anonymize this data using differential privacy[55] but you'll 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
  - Full list of optional diagnostic data: https://docs.microsoft.com/en-us/windows/privacy/windows-diagnostic-data
- MacOS:
  - More details on https://support.apple.com/guide/mac-help/share-analytics-information-mac-apple-mh27990/mac
- 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

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

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

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.

The WIFIs and Bluetooth devices around you:

Geolocation is not only done by using mobile antennas triangulation. It's also done using the WIFIs and Bluetooth devices around you. Operating systems makers like Google (Android[56]) and Apple (IOS[57]) maintain a convenient database of most WIFI 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) WIFI 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 can't really trust the settings. The whole operating system is built by a company that wants your data. Remember that if it's free then you are the product.

Don't take your smartphone with you where and when you are doing sensitive activities that you want to keep secret. Just don't. Leave it at home. Or if you absolutely have to take it with you, make sure it's powered off and consider the use of a faraday bag.

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's like knowing you had a call from an oncologist before then calling your family and friends successively. You don't know what was said during the conversation but you can guess what it was just from the "metadata"[58].

This metadata will also often include your location that is being harvested by Smartphones, Operating Systems (Android[59]/IOS), Browsers, Apps, Websites. Odds are there are several companies knowing exactly where you are at any time[60] because of your smartphone[61].

This location data has been used in many judicial cases[62] already as part of "geofence warrants" [63] 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.

Now let's say you're 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 can't trace back that VPN IP to your IP. Your ISP however knows (or at least has the ability to know) you were connected to that same VPN provider on November 4th from 7:30am to 2pm but doesn't know what you were doing with it.

The question is: Is there someone somewhere that would possibly have both pieces of information available[64] for correlation in a convenient database?

Have you heard of Edward Snowden[65]? Now is the time to google him and read his book[66]. I recommend reading about XKEYSCORE[67,68], MUSCULAR[69] and PRISM[70].

"We kill people based on Metadata"[71]

Your Smart devices in general:

You got it, your smartphone is an advanced spying device that:

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

All of this data is very likely being transmitted, processed and stored (unencrypted[72]) by various third parties.

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

- Your Smart Watch? (Apple Watch, Android Smartwatch …).
- Your Fitness Devices and Apps? (Strava[73,74], Fitbit[75], Garmin, Polar[76], …)[77]
- Your Smart Speaker? (Amazon Alexa[78], Google Echo, Apple Homepod …).
- Your Smart Transportation? (Car? Scooter?)

So when you're going to conduct anonymous or sensitive activities somewhere. Do not take your smart devices with you. Just don't and if you absolutely have to, make sure they're powered off and consider the use of a faraday bag.

Your Devices can be tracked even when completely powered off:

You've seen this in action/spy/Sci-Fi movies and shows, the protagonists always remove the battery of their phones to make sure it can't be used. Well this is now true at least for some devices:

- IPhones and IPads (IOS 13 and above)[79,80].
- Samsung Phones (Android 10 and above)[81].
- MacBooks (MacOS 10.15 and above)[82].

Such devices will continue to broadcast identity information to nearby devices even when off using Bluetooth Low-Energy[83]. They don't have access to the devices directly (which are not connected to the internet) but instead use BLE to find them through other nearby devices[84].

They can now locate such devices and keep the location in some database that could then be used by third parties or themselves for various purposes.

For this reason, you should not to bring your smartphone with you (even turned off) when you conduct sensitive activities. But if you absolutely have to take such devices with you, then you should again consider the use of a faraday cage around such devices in addition to turning them off.

Your RFID enabled devices:

RFID stands for Radio-frequency identification[85], it's 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[86]. 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 can't 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 and https://en.wikipedia.org/wiki/Radio-frequency_identification#Privacy

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[87].

Your Files Properties/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[88] 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's 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

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

On Windows I would recommend this NirSoft utility that allows you to view the EXIF data of pictures https://www.nirsoft.net/utils/exif_data_view.html. Alternatively on Windows and Linux I would recommend ExifTool that allows viewing AND editing those properties https://exiftool.org/.

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

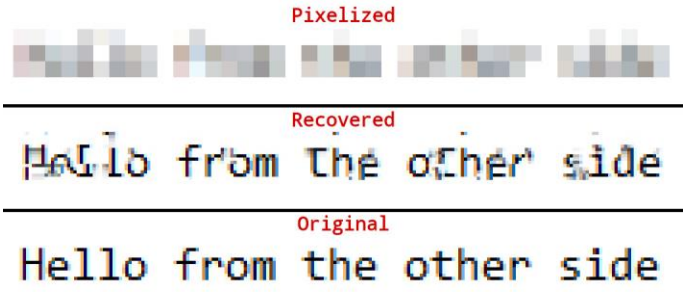
Here is a tutorial to remove metadata from a Picture using OS provided tools: https://www.purevpn.com/internet-privacy/how-to-remove-metadata-from-photos

Your Pixelized/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 actually 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



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 and I recommend for instance this interesting tutorial: https://medium.com/@somdevsangwan/unblurring-images-for-osint-and-more-part-1-5ee36db6a70b followed by https://medium.com/@somdevsangwan/deblurring-images-for-osint-part-2-ba564af8eb5d

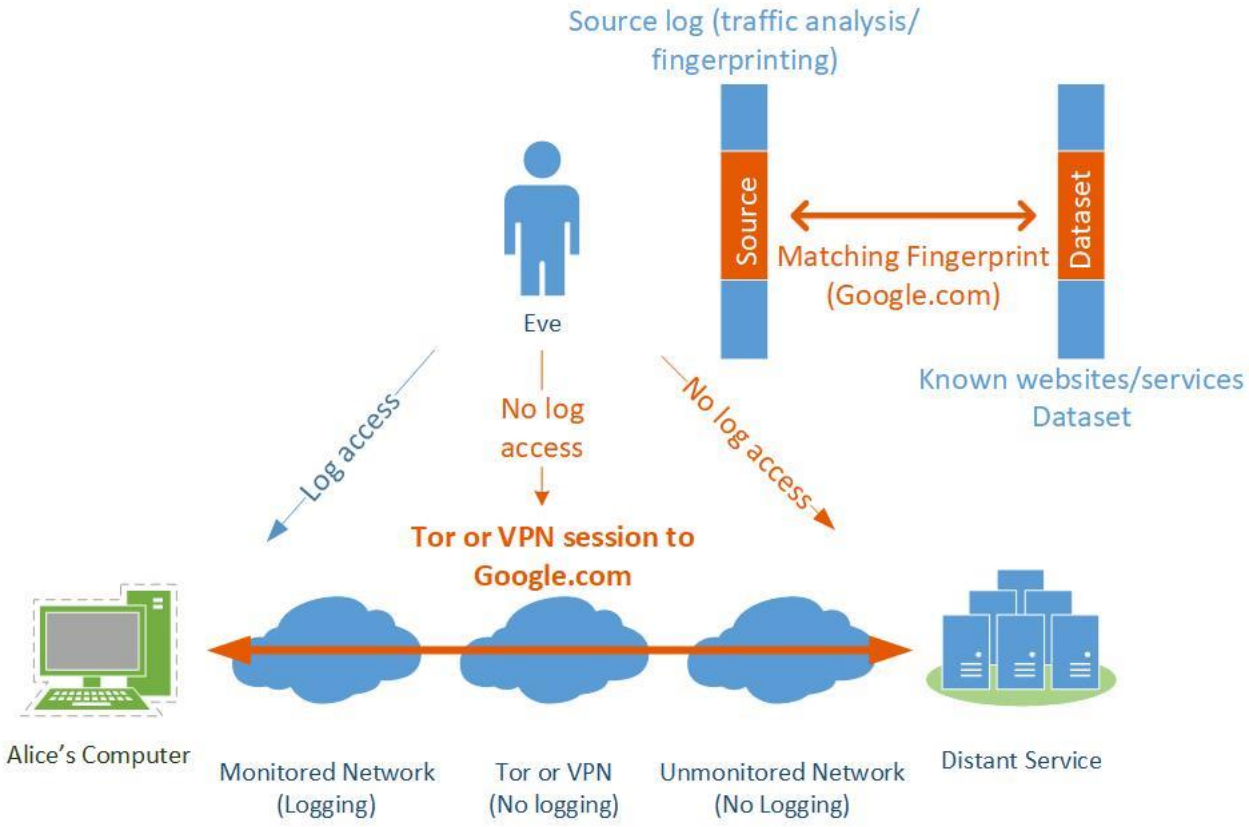
Last but not least you'll find plenty of deblurring resources here: https://github.com/subeeshvasu/Awesome-Deblurring

For this reason it's 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.

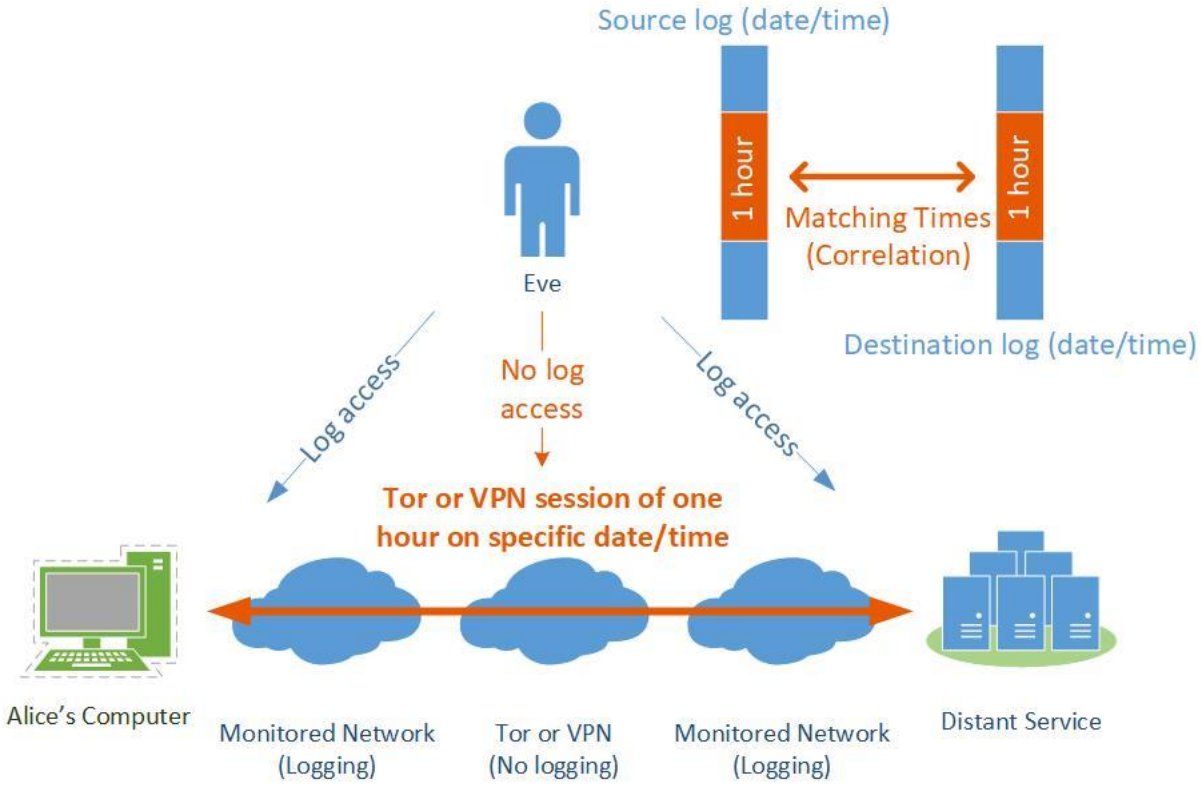
Your "Anonymized" Tor/VPN traffic:

Tor and VPNs are not silver bullets. Many advanced techniques have been developed and studied to de-anonymize encrypted traffic over the years[89]. 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:

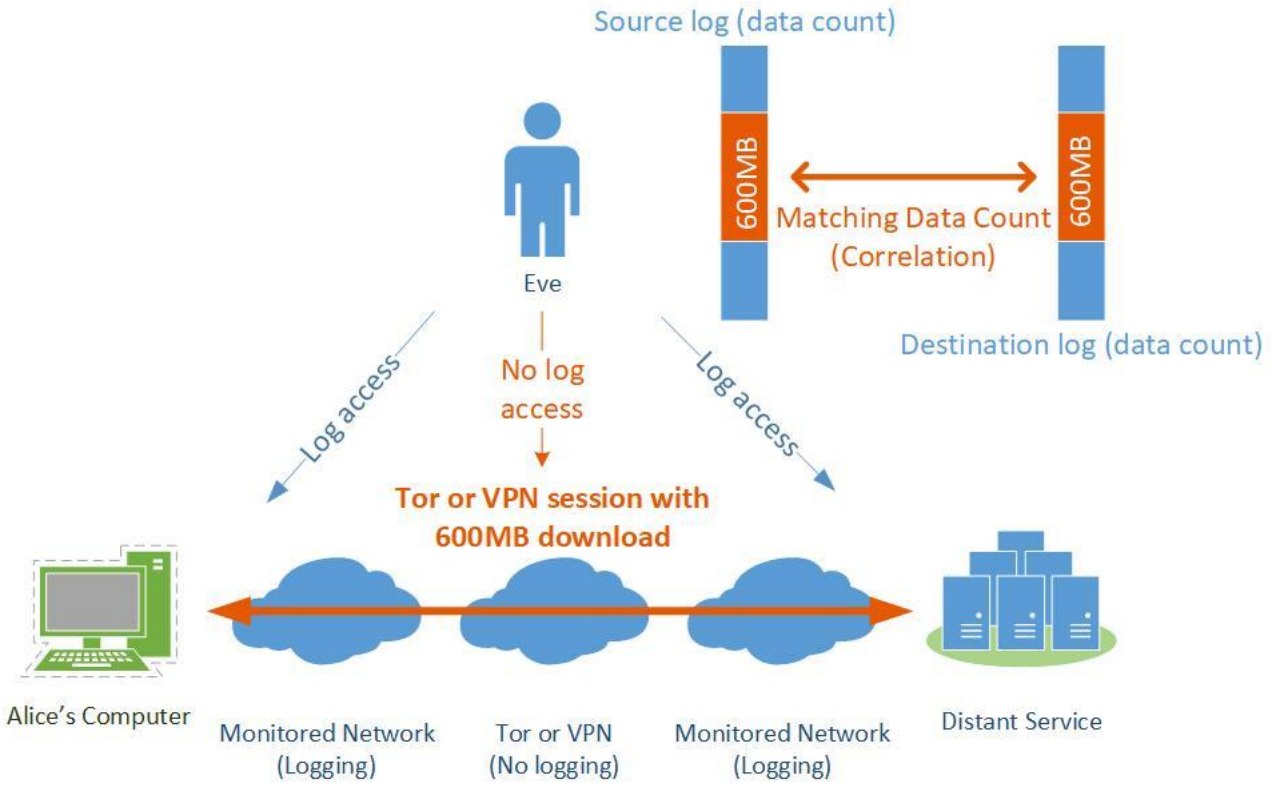
- Correlation Fingerprinting Attack: As illustrated (simplified) below, this attack will fingerprint[90] your encrypted traffic (like the websites you visited) just based on the analysis of your encrypted traffic (without decrypting it). It's able to do so with a whopping 96% success rate. Such fingerprinting 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).



- 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[91] a bomb threat hoax at Harvard University. It was also used to de-anonymize



- Correlation Counting Attacks: As illustrated (simplified) below, an adversary that has no access to detailed connection logs (can't 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 won't 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[92] with wide access to global mass surveillance (remember XKEYSCORE, MUSCULAR and PRISM). Such adversary might have access to logs no matter where you are and could use those to de-anonymize you.

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

(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 and specifically, "Part 3. Design goals and assumptions.".)

Lastly, do remember that using Tor in itself can already be considered a suspicious activity[93] and it's use could be considered malicious by some[94].

We will later propose a propose a multi-layered approach over a combination of Tor and VPN as well as using public Wi-Fi over a known internet connection.

Your Crypto transactions:

Contrary to popular belief, Crypto transactions (such as Bitcoin and Ethereum) are not anonymous[95]. Most crypto currencies can be tracked accurately through various methods[96].

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'll 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[97] financial regulations) and can then trace back those crypto transactions to you using the financial system.

There are some crypto currencies with privacy in mind like Monero but even those can be de-anonymized to some extent[9899].

Even if you use Mixers or Tumblers (services that specialize in anonymizing crypto currencies by "mixing them"), keep in mind this is only obfuscation and not actual anonymity[100].

Exploits in your apps:

So you're using Tor Browser or Brave Browser with a Tor Tab. You could be using those over a VPN for added security. But you should keep in mind that there are exploits[101] (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[102] case in 2013 where the FBI inserted malware[103] using a Firefox browser exploit on a Tor website. This exploit allowed them to reveal details of some users.

Here are some steps to mitigate this type of attack:

- You should never have 100% trust in the apps you're using.
- You should always check that you're using the updated version of such apps before use.
- You should not use such apps directly from a hardware system but instead use a Virtual Machine.

To reflect these recommendations, this guide will therefore later guide you in the use of Virtualization so that even if your Browser/Apps get compromised by a skilled adversary, that adversary will find himself stuck in a sandbox[104] without being able to access identifying information.

Your CPU:

All modern CPUs[105] are now integrating hidden management platforms such as the now infamous Intel Management Engine[106] and the AMD Platform Security Processor[107].

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 videos: BlackHat, How to Hack a Turned-Off Computer, or Running Unsigned Code in Intel Management Engine https://www.youtube.com/watch?v=mYsTBPqbya8

These have already been affected by several security vulnerabilities in the past[108] 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[109].

There are some not so easy ways[110] 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.

We will try to mitigate this issue 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 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 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[111], Cellebrite Cloud[112]) that will help an adversary analyze your cloud data with ease.

Notable Examples:

- Apple ICloud: https://support.apple.com/en-us/HT202303 : "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/ : "**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 "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 : 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**."

Generally speaking, you should not trust cloud providers with your 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.

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

Your Digital Fingerprint and Footprint:

The digital fingerprint is the way you write, the way you behave. The way you click. The way you browse. The fonts you use on your browser[113]. 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.

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 don't send it / save it. Think of when you write an e-mail in Gmail. It's saved automatically as you type. They can register your clicks and cursor movements as well.

This technology is also widely used used in CAPTCHAS[188] 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's unclear if such data is used or not by Governments and Law Enforcements agencies but it might be in the

future. And while this might only be used for advertising/marketing purposes now. It could and probably will be used for investigations in the short or mid-term future.

Your Clues about your Real Life:

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[114] who shared over time several details about his past and was later discovered.

There are also a few cases involving OSINT at Bellingcat[115].

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

Your Browser and Device Fingerprints:

Your Browser and Device Fingerprints[198] 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're 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[116] based browsers (such as Chrome) or Firefox[117] unless taking special measures.

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

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

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 didn't 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.

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/

This guide will mitigate these issues by mitigating, obfuscating and randomizing many of those fingerprinting identifiers by using Virtualization and also using by fingerprinting resistant Browsers.

Note that

Your Face and other Biometrics:

Hell is other people. Even if you evade every methods listed above, you're 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[118,119] and have been using other means (Satellite imagery) to create maps of "people" around the world[120].

If you are walking in a touristy place, you'll 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 doesn't provide a timestamp and geolocation, it can still be guessed with other means[121,122].

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/
- 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/
- 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/
- Bellingcat, Advanced Guide on Verifying Video Content https://www.bellingcat.com/resources/how-tos/2017/06/30/advanced-guide-verifying-video-content/

Even if you're not looking at the camera, they can still figure out who you are[123] and even make out your emotions[124].

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[125,126,127,128,129].
- 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.

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 provider by private companies such as the Israeli AnyVision[130]) in their CCTV networks to look for "persons of interest"[131]. And some heavily surveilled states like China have implemented widespread use of Facial Recognition for various purposes[132] including possibly identifying ethnic minorities[133].

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.

We can safely imagine a near future where you won't be able to create accounts or sign-in anywhere without providing unique biometrics (A good time to re-watch Gattaca[134], Person of Interest[135] and Minority Report[136]).

At this time, there are a few steps[137] 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[138].
- 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 eyes features.

(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:

Phishing[139] is a type of attack where an adversary could try to extract information from you by pretending to be something/someone else.

A typical case is an adversary using a man-in-the-middle[49] attack or a falsified e-mail/call to ask your credential for a service. This can be your e-mail or your financial services for example.

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

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-luNA

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're encrypted[140]. 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/
- New-York Times, The Police Can Probably Break Into Your Phone https://www.nytimes.com/2020/10/21/technology/iphone-encryption-police.html
- Vice, Cops Around the Country Can Now Unlock iPhones, Records Show https://www.vice.com/en/article/vbxxxd/unlock-iphone-ios11-graykey-grayshift-police

When it comes to your laptop, the forensics techniques are many and widespread. Too many to be listed in this guide. But this guide will nonetheless guide you into mitigating most forensic techniques and hopefully help you protect yourself from "most" adversaries.

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[141] or a national security letter[142]) log your activity to de-anonymize you. There have been several recent examples of those:

- 2020, The Germany based mail provider Tutanota was forced to implement a backdoor to save unencrypted copies of the e-mails of one user[143].
- 2017, PureVPN was forced to disclose information of one user to the FBI[144].
- 2014, EarthVPN user was arrested based on logs provider to the Dutch Police[145].
- 2014, HideMyAss user was de-anonymized and logs were provider to the FBI[146].
- 2013, Secure E-Mail provider Lavabit shuts down after fighting a secret gag order[147].

Some providers have implemented the use of a Warrant Canary[148] 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.

Last but not least, it's now well known that some companies might be sponsored front-ends for some state adversaries(see the Crypto AG story[149] and Omnisec story[150]).

For these reasons, it's important that you don't 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 I will recommend the use of a cash-paid VPN provider over Tor to prevent the VPN service from knowing any identifiable information about you. I will also recommend the creation of anonymous e-mail accounts from this VPN over Tor connection to also prevent them from having any information despite their no logging policies.

Advanced targeted techniques:

There are many advanced techniques that can be used by skilled adversaries[151] 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 (Air-Gap Research Page, Cyber-Security Research Center, Ben-Gurion University of the Negev, Israel). I recommend having a look if you're curious.

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

This guide will be of little help against such adversaries.

Notes:

If you still don't 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 won't count things like PRISM, MUSCULAR or XKEYSCORE explained earlier:

- Google Transparency Report https://transparencyreport.google.com/user-data/overview
- Facebook Transparency Report https://transparency.facebook.com/
- Apple Transparency Report https://www.apple.com/legal/transparency/
- Cloudflare Transparency Report https://www.cloudflare.com/transparency/
- Snapchat Transparency Report https://www.snap.com/en-US/privacy/transparency
- Telegram Transparency Report https://t.me/transparency (requires telegram installed)
- Microsoft Transparency Report https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report
- Amazon Transparency Report https://www.amazon.com/gp/help/customer/display.html?nodeId=GYSDRGWQ2C2CRYEF
- Dropbox Transparency Report https://www.dropbox.com/transparency
- Discord Transparency Report https://blog.discord.com/discord-transparency-report-jan-june-2020-2ef4a3ee346d
- GitHub Transparency Report https://github.blog/2020-02-20-2019-transparency-report/
- Snapchat Transparency Report https://www.snap.com/en-US/privacy/transparency/
- TikTok Transparency Report https://www.tiktok.com/safety/resources/transparency-report?lang=en
- Reddit Transparency Report https://www.reddit.com/wiki/transparency
- Twitter Transparency Report https://transparency.twitter.com/

General Preparations:

Picking your 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 laptop for your anonymous activities:
  - But it's old, slow and has bad specs (<6GB of RAM, less than 250GB disk space, old/slow CPU)
    - **You should go for the TAILS route.**
  - It's not that old and it has decent specs (=> 6GB of RAM, 250GB of disk space or more, decent CPU)
    - **You could go for TAILS, Whonix routes.**
  - It's new and it has great specs (>8GB of RAM, >250GB of disk space, recent fast CPU)
    - **You could go for TAILS, Whonix or Qubes.**

Skills:

- You have no IT skills at all and this guide looks like an alien language to you?
  - **You should go with the TAILS route.**
- You have some IT skills and mostly understand this guide so far
  - **You should go with TAIL or Whonix routes.**
- You have moderate to high IT skills and you already knew much of what's in this guide
  - **You should go with anything you like including Qubes.**
- You are a l33T hacker, there is no spoon, the cake is a lie
  - **This guide is not for you**

Adversaries (threats):

- If your main concern is forensic examination of your devices:
  - **You should go with the TAILS route.**
- If your main concerns are remote adversaries that might uncover your online identity in various platforms:
  - **You should go with the Whonix or Qubes routes.**

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/Dev/Threat_Model
- https://www.whonix.org/wiki/Comparison_with_Others

Steps for all routes:

Get a burner phone:

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

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 allows 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 WIFI.

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's really important that you leave your smartphone at home when going (or turn it off before leaving if you have to keep it) and that you test the phone at a random location that cannot be tracked back to you (and again, don't do that in front of a CCTV, avoid cameras, be aware of your surroundings). No need for WIFI 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:

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

This is the hardest part of the whole guide and also its biggest weakness. It's a SPOF (Single Point of Failure). The places where you can still buy prepaid SIM cards without ID registration are getting more and more limited due to various KYC type regulations[152]. But this is unfortunately a required step as you will NEED a reliable phone number to sign-up for many accounts.

There are many commercial services offering numbers to receive SMS messages online but those have basically no anonymity 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. To this date, I do not know any reputable service that would offer this service and accept cash payments (by post for instance).

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. This is mainly because again Bitcoin and crypto are mostly NOT anonymous and transactions can be traced and tracked back to you in various ways.

In the end, it's probably just more convenient, cheaper and less risky to just get a pre-paid SIM card from one of the places who still sell them for cash without requiring ID registration. So here is a list of places where you can still get them at the moment: https://prepaid-data-sim-card.fandom.com/wiki/Registration_Policies_Per_Country

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). Don't forget to not have your smartphone with you or if really have to powered off before going at the point of sale. Try to avoid CCTV and cameras and don't forget to buy a Top Up voucher with the SIM card (if it's not a package) as most pre-paid cards will require a top-up before use.

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're "affordable", do not require identification for activation and top-pup 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're 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.

Get an USB key:

Get at least one decent size USB key (at least 16GB).

Find some safe places with decent public WIFI:

You need to find safe places where you'll be able to do your anonymous activities using some publicly accessible WIFI (without any account/ID registration, avoid CCTVs).

This can be anywhere that won't be tied to you directly (your home/work) and where you can use the WIFI 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'll need to buy a coffee to get the WIFI access code in most. If you pay this coffee with an electronic method, they will be able to tie your WIFI 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 won't be available yet to your local cops, 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.

The TAILS route:

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

- You can't 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[153] stands for **The Amnesic Incognito Live System.** . It's 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.

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.

It does however have some drawbacks:

- Tails uses Tor and therefore you'll 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's yours or some public Wi-Fi) will also see that you're using Tor and this could make you suspicious in itself.
- Tails doesn't 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's very secure will be detected as well by most platforms and will hinder you in creating anonymous identities on many platforms.
- Tails won't protect you more from the 5$ wrench[5].
- Tor in itself might not be enough to protect you from an adversary with enough resources as explained earlier.

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

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

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

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

Steps for all other routes:

Get a laptop for your anonymous activities:

Ideally (but not mandatory[154]), you should get a dedicated that won't be tied to you in any easy way laptop (paid with cash anonymously as previously mentioned for the phone and the SIM card).

This laptop should be in all cases a clean freshly installed PC (Running Windows/Linux). This laptop should be clean of your normal day to day activities. In the case of a Windows laptop, and if you used it before, it should also not be activated (installed without a product key).

This is to mitigate 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.

The laptop should have at least 250GB of Disk Space **at least 6GB** 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.

Ideally (but not mandatory) this laptop should have an HDD and not an SSD for reasons that will explained later.

This laptop should ideally (but not mandatory for the same reason as above) never have been connected to your known networks at this stage. This is because it's possible your laptop already sent out telemetry data or activation data to a third party (like Microsoft) that could include network information, activation information and/or location data.

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.

A note for Linux users to avoid wasting your time later:

Your Linux laptop should have full disk encryption enabled from the start. This process can be tedious if you intend to do this after installation depending on your distribution.

You should consider re-installing your Linux laptop at this stage if it's not encrypted.

In the case of Ubuntu, the process is explained in details in this tutorial:
https://help.ubuntu.com/community/Full_Disk_Encryption_Howto_2019

Bios/UEFI Settings of your laptop:

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

Once you're in there you'll need to apply a few recommended settings:

- Disable Bluetooth completely if you can.
- Disable Biometrics (fingerprint scanners) if you have any and if you can.
- Disable the Webcam and Microphone if you can.
- Enable BIOS/UEFI password and use a long passphrase[155] instead of a password if you can.
- Disable USB/HDMI or any other port (Ethernet, Firewire, SD card …) if you can.

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).

Tamper protect your laptop:

At some point you'll inevitable leave this laptop alone somewhere. You won't 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 won't use a 5$ wrench against you[5].

It's important to know that it's 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/ [156] (with pictures).

Check the 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[157], they'll require a host OS to run the Virtualization software. You have two choices in this part of the guide:

- Your Linux distribution of choice (excluding Qubes)
- Windows 10 Home edition

Linux is not necessarily the better choice for privacy depending on your threat model. This is because using Windows will allow us to use a privacy feature called Plausible Deniability[158].

So what is Plausible Deniability? Plausible deniability is the ability for you to cooperate with an adversary requesting access to your device/data without revealing your true secret.

A (nice) 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 not incriminate yourself") but some countries are implementing laws[159] 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 comes 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's 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 is only (easily) available with Windows and is a reason why you might want to use Windows instead of Linux.

Plausible deniability is also the reason you should have Windows 10 Home (and not Pro) on your laptop. This is because Windows 10 Pro natively offers a full-disk encryption system (Bitlocker[160]) 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.

Also if you have zero knowledge of Linux, I would recommend you go for Windows instead for convenience. This guide will help you hardening it as much as possible to prevent any leaks.

In all cases, the host OS will never be used to conduct anonymous activities. The host OS network will only be used to connect to a Wi-Fi Access Point. It will be left unused during the whole duration of the process and should not be used for any of your known activities.

Enable MAC address randomization on your laptop:

You need to follow these steps to randomize your MAC address as explained earlier in this guide:

- Windows 10:
  - Go into Settings > Network & Internet > Wi-Fi > Enable Random hardware addresses
- Linux:
  - Ubuntu, follow these steps https://help.ubuntu.com/community/AnonymizingNetworkMACAddresses
  - Any other distro: you will have to find the documentation yourself but it should be quite similar to the Ubuntu tutorial.

Setting up a safe Browser on your Host OS:

This guide will 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 themselves recommend the use of Tor Browser if you feel your safety depends on being anonymous[161]: " With Tor, Brave works hard to ensure that you're extremely difficult to track online while providing a delightful browsing experience. But if your personal safety depends on remaining anonymous you may wish to use the Tor Browser instead. ".

This Browser on the host OS will only be used to download various utilities and will never be used for actual anonymous activities.

- Download and install Tor Browser from https://www.torproject.org/download/
- Open Tor Browser

Go to next step and use this browser for all the next steps within the host OS unless instructed otherwise.

Enable some additional privacy settings on your Host OS:

Windows:

See Appendix B: (Windows Additional Privacy Settings)

Linux:

- Ubuntu 18+: Just make sure you didn't enable any telemetry and follow this tutorial if needed https://vitux.com/how-to-force-ubuntu-to-stop-collecting-your-data-from-your-pc/
- Any other distro: You'll need to document yourself and find out yourself how to disable telemetry if there is any.
- Apply the same nextdns.io recommendations as in the Windows section above. Use their Linux setup guide instead.

Windows Host OS encryption:

Skip this if you decided to go for a Linux Host OS instead.

Go ahead and download and install Veracrypt from: https://www.veracrypt.fr/en/Downloads.html

Veracrypt[162] is the software we will use 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's 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's 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[163] encryption software that also provides plausible deniability for general use.

But there are catches as there are with everything:

Evil-Maid Attacks:

The first catch is called the "Evil Maid Attack"[164]. This is when someone tampers with your laptop while you're away. For install to clone your hard drive or to install a key logger. If they are able to 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 within your laptop (software or hardware), they will be able to simply get the password from you for later use when they seize it. 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 won't 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.

In addition, Veracrypt itself has a built-in protection against Evil Maid Attacks that should detect a modified bootloader (a software malware) that could try to log your password.

Cold-Boot Attack:

The second catch is the "Cold Boot attack"[165] discussed briefly earlier in this guide. This is trickier than the Evil Maid Attack as it requires them to come into possession of your laptop while you're actively using the hidden OS/data or very shortly afterward.

The principle is simple, as shown in this video[166], they could theoretically quickly boot your laptop on a special USB key that would copy the content of the RAM (the memory) of the laptop 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). The memory won't decay and they could be able to copy its content for analysis. This memory dump should contain the key to decrypt your hard drive/data. To mitigate this you have to apply a few principles:

- Encrypt the memory with a Veracrypt option[167] (settings > performance/driver options > encrypt RAM) at a cost of 5-15% performance. This will also disable hibernation.
- 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[168].
- Be careful and have a good situational awareness when using your hidden system, if you sense something weird. Shut your laptop down as fast as possible.

There have been some forensics studies[169] 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[170] and by the maintainer of Veracrypt[171].

Local Data leaks (traces) and forensics examination:

This last catch applies mostly to encrypted file containers vs full disk encryption. These are data leaks and traces from your operating system and apps when you access "hidden files" from your computer.

Let's say you have a Veracrypt encrypted USB key or External and plausible deniability enabled.

Depending on the password you use when mounting the drive, it will open a decoy folder or the sensitive folder. Within those folders, you'll have decoy documents/data within the decoy folder and sensitive documents/data within the sensitive folder.

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

Well, all those Apps and your Operating System will 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 Windows file indexing system that could index the drive, thumbnails that could be generated …

A very good example of this are the Windows "ShellBags" that are stored within the Windows Registry storing various histories of accessed files/folders[172].

Forensics can[170] and will[172] use all those leaks[168] to prove the existence of hidden data and defeat your attempts at using plausible deniability.

It will be therefore important to apply various steps to prevent forensics from doing this by preventing and cleaning these leaks/traces. This will be covered in the "Cover your Tracks" part of this guide at the very end.

Online data leaks:

Whether you're 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 (whether it's a Hidden Operating System or a Hidden Volume).

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 easily be used to prove the existence of a hidden OS / Volume on a computer and would be readily available at Microsoft. Therefore it's critically important that you disable and block telemetry with all the means at your disposal as instructed in this guide earlier in the Privacy Settings chapter.

Deciding which sub-route you'll take:

Remember that plausible deniability is not a silver bullet and will be of little use in case of torture[5]. As a matter a fact, depending on who your adversary would be (your threat model), it might be wise not to use Veracrypt at all as shown in this demonstration: https://defuse.ca/truecrypt-plausible-deniability-useless-by-game-theory.htm

Now you'll have to pick your next step between two options:

- Route A: Simple encryption of your current OS
    - Pros:
        - Doesn't 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:
        - Doesn't 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'll 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 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[173] Operations[174]. This will severely degrade the performance/health of your SSD drive over time.

As you can see, Route C really only offers two privacy advantages over the others and it will only be of use against a "soft" (lawful and nice) adversary.

Deciding which route you'll 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 bootloop.

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 actually using your laptop's keyboard (AZERTY for example) as you'll 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 (Windows tutorial)

You don't have to have an HDD for this method and you don't 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 won't 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)[155]
- Collect some entropy by randomly moving your cursor around until the bar is full
- Click Next as the Generated Keys screen
- To rescue disk[175] or not rescue disk, well that's 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'll 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[176] 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 has to pass in order 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're 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)

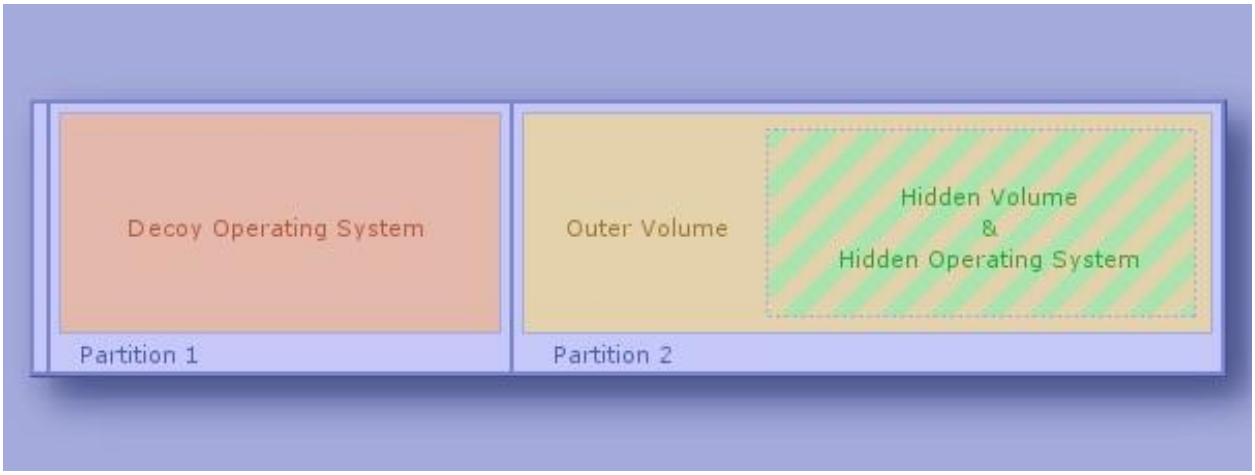
This is only supported on Windows.

This is only recommended on an HDD drive. This is not recommended on an SSD drive.

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 (Process of Creation of Hidden Operating System part) and https://www.veracrypt.fr/en/Security%20Requirements%20for%20Hidden%20Volumes.html (Security Requirements and Precautions Pertaining to Hidden Volumes).

This is how your system will look after this process is done:



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[177] (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 have to do it to prevent data leaks[178] that could allow forensics to defeat your plausible deniability[179][180]. 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

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
    - 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[155]
- 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 a 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 don't fill the outer volume too much or too little (about 40%). Remember you have to leave enough space for the Hidden OS (which will be same size as the first partition you created during installation).
- Use a strong passphrase[155] 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
- 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[181] or not rescue disk, well that's 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'll 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 has to pass in order 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.

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

You should do this from a safe trusted place.

Basically you're 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 have to make the Decoy OS as plausible as possible. We also want your adversary to think you're not that smart.

Therefore it's 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

- **You are using Veracrypt because you are using Windows 10 Home which doesn't 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 don't want anyone in your entourage to see your stuff. And so you didn't 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 anonymous activities in itself, 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.**

You're done and can go to next step.

Virtualbox:

This step and the following steps should be done from within the Host OS. This can either be your Host OS with simple encryption or your Hidden OS with plausible deniability.

In the Whonix route, we will make extensive use of the free Oracle Virtualbox[182] 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 KVM in Linux, feel free to do so).

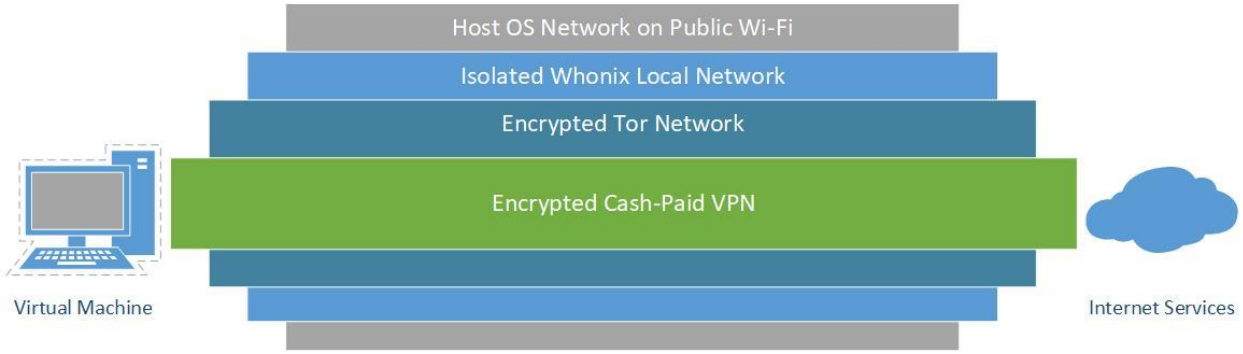
All your hidden anonymous activities will be done from within a client Virtual Machine running Windows 10 Pro (not Home this time) or Linux.

This has a few advantages that will greatly help you remain anonymous:

- It will prevent the client VM OS (Windows/Linux), 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 has to go through Tor no matter what.

There will be two possibilities here, one without a cash-paid VPN and one with added cash-paid VPN.

As you can see in this illustration, if your cash-paid VPN is compromised by an adversary (despite their privacy statement and no-logging policies), they will only find an anonymous cash-paid account connecting to their services from a Tor Exit node.



If they somehow also manage to compromise the Tor network, they will still be faced with the internal IPs of a random public Wi-Fi that is not tied to your identity.

If they somehow compromise your VM OS (with a malware), they will be faced with an internal IP of the Virtual Machine and won't be able to figure out the Public Wi-Fi IP.

This other illustration shows the other possibility without a cash-paid VPN. It's very similar but has one less defense layer. If the Tor network is compromised by a Global/State actor, then you will be likely de-anonymized quickly.

In addition, using Tor will raise the suspicion of many platforms. You will face many hurdles (captchas, errors, difficulties signing-up) if you use Tor directly.

For these reasons, I strongly recommend the VPN over Tor solution.

This multi-layered approach should greatly reduce the odds of your adversaries being able to de-anonymize you easily.

You might be wondering: Well what about using Tor over VPN instead of VPN over Tor? Well this is not recommended because:

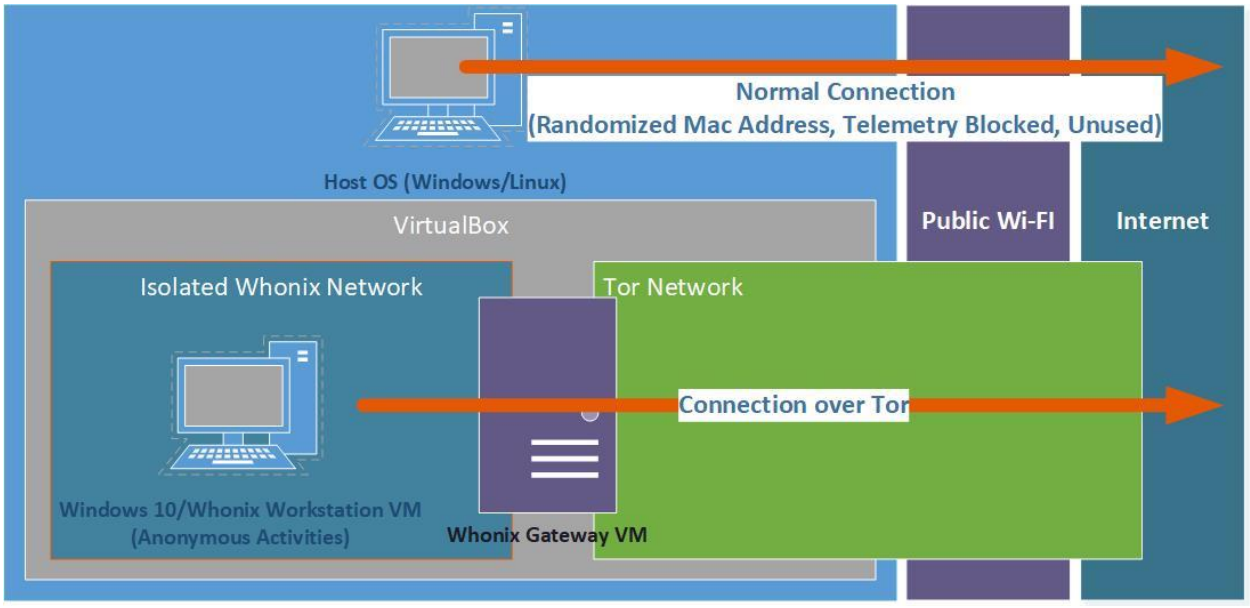
- Your VPN provider is just another ISP that will then know your origin IP and will be able to de-anonymize you with ease. We don't trust them.
- This would result in you connecting to various services using the IP of a Tor Exit Node which are banned/flagged in many places.

This route will use Virtualization and Whonix[183] as part of the anonymization process. Whonix is a Linux distribution composed of two Virtual Machines:

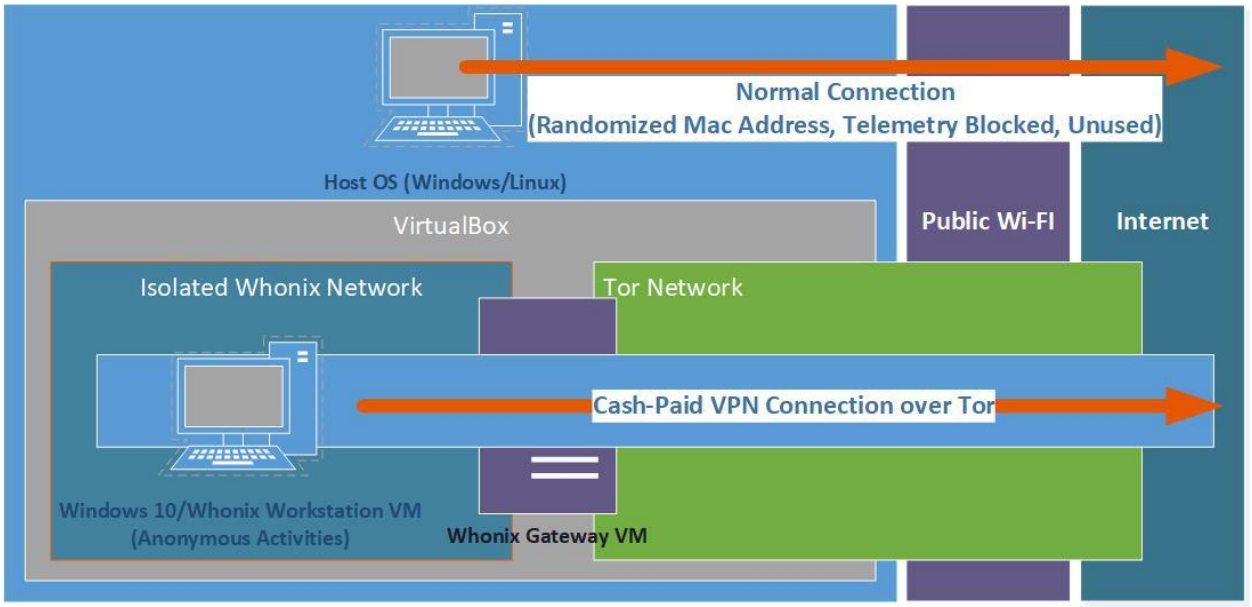
- The Whonix Workstation (this is a VM where you can conduct anonymous activities)
- The Whonix Gateway (this VM will establish a connection to the Tor network and route all the network traffic from the Workstation through the Tor network).

This guide will therefore propose 2 flavors of this route:

- The Whonix only route where all traffic is routed through the Tor Network



- A Whonix hybrid route where all traffic is routed through a cash-paid VPN over the Tor Network



You will be able to decide which flavor to use based on my recommendations. I strongly recommend the second one.

Whonix is well maintained and has extensive documentation.

A note on Virtualbox Snapshots:

Later on you will create and run several Virtual Machines within Virtualbox for your anonymous activities. Virtualbox provides a feature called "Snapshots"[184] 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 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 "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 won't 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[185]. Fortunately there will be ways to remove those traces after deletion or reverting to a previous snapshot. Such techniques will be discussed in the "Cover your tracks" section of this guide.

You may now go ahead and download Virtualbox from https://www.virtualbox.org/wiki/Downloads

Then install Virtualbox on your Host OS and go to next step.

Get an anonymous (cash-paid) VPN subscription:

If you follow my advice, you will also need a VPN subscription but this time you will need an actually anonymous one that can't be tied to you by the financial system. Meaning you will need to buy a VPN subscription with cash. You will later use this VPN to connect to the various services anonymously but never directly from your IP.

There are three VPN companies recommended by privacytools.io (https://privacytools.io/providers/vpn/) that accept cash payments: Mullvad, IVPN and ProtonVPN.

Personally I would recommend Mullvad due to personal experience.

How does this work?

- Open or Tor 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.

- 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.
- Wait for them to receive the payment and enable your account (this can take a while).
- Connect to your VPN again.
- Open Tor Browser.
- Check your account status and proceed when your account is active.

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 within a Virtual Machine in a secure way as we don't trust VPN providers "no logging policies". This VPN provider should never know your origin IP.

Download various utilities:

You should download a few things within the host OS.

- The latest version of the Virtualbox installer for Windows X64
- The latest Whonix OVA file from https://www.whonix.org/wiki/Download 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.

Whonix Virtual Machines:

- Start Virtualbox on your Host OS.
- Import Whonix file Into Virtualbox following the instructions on https://www.whonix.org/wiki/VirtualBox/XFCE
- Start the Whonix VMs
- Update the Whonix VMs following the instructions on https://www.whonix.org/wiki/Operating_System_Software_and_Updates#Updates
- 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

Note: You should also read these very good recommendations over there https://www.whonix.org/wiki/DoNot as most of those principles will also apply to this guide.

Windows 10 Virtual Machine:

This step is optional. You can decide if you prefer to conduct your anonymous activities from a Windows VM that will use the Whonix Gateway or if you will just use the Whonix Workstation provider earlier.

Using Whonix will require more skills on your side as it is a Linux distribution. You will also encounter more difficulties if you intend to use specific software that might be harder to use on Whonix. In addition, Whonix will only run Tor Browser where the Windows VM will allow you to easily run a different Browser (such as Brave). Using Tor Browser will significantly increase your difficulty in creating online identities on many online platforms.

Setting up a VPN over Tor on Whonix will also be much more complicated than on Windows as well.

If you have zero knowledge with Linux, I would suggest a hardened Windows VM for the sake of simplicity.

- If you want to use Whonix, you should skip this next section.
- If you want to use Windows, please follow those steps:

Windows 10 ISO download:

See "Appendix C: (Windows Installation Media Creation)" and go with the ISO route.

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 won't reach that much)
- Select the VM and click Settings, Go into the Network Tab
- Select "Internal Network" in the "Attached to" Field
- 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)"
- 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
    - Gateway 10.152.152.10 (this is the Whonix Gateway)
    - DNS 10.152.152.10 (this is again the Whonix Gateway)
    - Save
- 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 instead of Tor Browser. The reasons are:

- You will encounter far less issues later with account creations (captchas …).
- You will enjoy ad-blocking where none is available in Tor Browser.
- The whole traffic will be router over a VPN over Tor anyway.
- Performance is far better than Tor Browser

But again, if you are extra paranoid and want to use Tor Browser and have "Tor over VPN over Tor", you should skip this step and go with Tor Browser within the VM as well.

If you want to use Brave:

- Download and install Brave browser from https://brave.com/download/
- 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

Additional Privacy settings in Windows 10:

See “Appendix B: (Windows Additional privacy settings)”

VPN client installation (cash-paid):

If you decided to not use a cash-paid VPN and just want to use Tor, skip this step.

Download the VPN client installer of your cash paid VPN service and install it on the VM of your choice (Windows or Whonix).

- Whonix Tutorial (should work with any VPN provider): https://www.whonix.org/wiki/Tunnels/Connecting_to_a_VPN_before_Tor
- Windows Tutorials:
  - Mullvad: https://mullvad.net/en/help/install-mullvad-app-windows/
  - IVPN: https://www.ivpn.net/apps-windows

In both cases you should set the VPN to start from boot and enable the “kill switch” if you can.

- Windows: https://mullvad.net/en/help/using-mullvad-vpn-app/#killswitch
- Whonix: Coming Soon, I didn’t find a suitable tutorial yet.

KeePassXC:

You will need something to store your data (logins/passwords, identities and TOTP[186] information).

For this purpose I strongly recommend KeePassXC because of their TOTP feature. This is the ability to create entries for 2FA[187] authentication with the authenticator feature.

Here are the tutorials:

- Whonix: https://www.whonix.org/wiki/KeePassXC
- Windows: https://KeePassXC.org/docs/KeePassXC_GettingStarted.html#_microsoft_windows

Test that KeePassXC is working before going to next step.

You are done and can now skip the rest to go to the “Creating your anonymous online identities” part.

The Qubes Route:

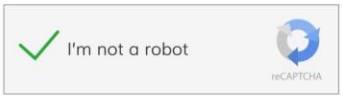
Coming Soon.

Creating your anonymous online identities:

Understanding the methods used to prevent anonymity and verify identity:

Captchas:

Captcha[188] stands for “Completely Automated Public Turing test to tell Computers and Humans Apart” are Turing tests[189] puzzles you need to complete before accessing a form/website. You’ll mostly encounter those provided by Google (reCaptcha service[190]) and Cloudflare (hCaptcha[191]). hCaptcha is used on 15% of the internet by their own metrics[192].



They're designed to separate bots from humans but in reality are also used to deter anonymous and private users.

If you frequently use VPNs, you'll quickly encounter many captchas everywhere. Quite often when using Tor, even if you succeed in solving all the puzzles, you'll still be denied after solving the puzzles.

While most people think those puzzles are only about solving a little puzzle, it's important to understand that it's much more complex and that modern Captchas uses advanced machine learning and risk analysis algorithms to check if you're human[193]:

- They check your browser, cookies and browsing history using Browser fingerprinting[194].
- They track your cursor movements (speed, accuracy) and use algorithms to determine if it's "human".
- They track your behavior before/during/after the tests to ensure you're "human"[195].

It's 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 and sometimes very difficult ones involving reading undecipherable characters or identifying various objects on endless pictures set. You'll also have more captchas if you use ad blocking system or if your account was flagged for any reason for using VPNs or Tor previously.

You'll also have (in my experience) more Captchas (reCaptcha) in Google if you don't use Chrome. But this can be mitigated by using Chromium based browsers such as Brave. There is also a Browser extension called Buster that could help you those https://github.com/dessant/buster.

As for Cloudflare (hCaptcha), you could also use their Accessibility solution here (https://www.hcaptcha.com/accessibility) 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"[196] https://privacypass.github.io/ 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're solving them (speed/movement/accuracy/…) as to prevent "Captcha Fingerprinting".

Fortunately as far as I'm aware, these are not yet officially/publicly used to de-anonymize users for third parties.

Phone verification:

Phone verification is advertised by most platforms as a way to verify you're human. But don't be fooled, the main reason for phone verification is not only to check if you're 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[197].

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 won't allow you to register using an IP address from the Tor network.

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.

User details checking:

Obviously, Reddit doesn't 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?
- Details unknowns in their contact discovery service? (Meaning nobody else knows you?)
- Locking down privacy settings after signing-up?
- Name that doesn't 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 …).

This is a line I'm not going to help you cross. I just strongly think platforms doing this are *bad actors* and are clearly 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.

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 before 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's 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. 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're not considered "open proxies" but that won't 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[198] Fingerprinting are usually integrated into the Captcha services but also in other various services.

Many platforms (like Google[199]) will check your browser for various capabilities and settings and block Browsers they don't like. This is one of the reasons I recommend using Brave Browser over Tor Browser within your 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 is able to 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're 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: Similar to the Canvas and WebGL fingerprints these will fingerprint your audio capabilities.
- CPU: What kind of CPU you're 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.
- …

Here are two services you can use to check your browser Fingerprinting:

- https://coveryourtracks.eff.org/
- https://amiunique.org

Chances are you'll 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'll want to verify that you exist by asking you to reply to an e-mail/chat/phone call.

It's annoying but very easy to deal with in our case. We're 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 doesn't matter when you're 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:

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

Financial transactions:

Simple and efficient, some platforms will require than you perform some kind of financial transaction to verify your account. 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.

Again this is just a way for them to delegate the user verification on the financial system.

Sign-in with some platform:

Why do this user verification ourselves when we can just ask others to deal with it?

You’ll 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[200] and unfortunately sometimes required.

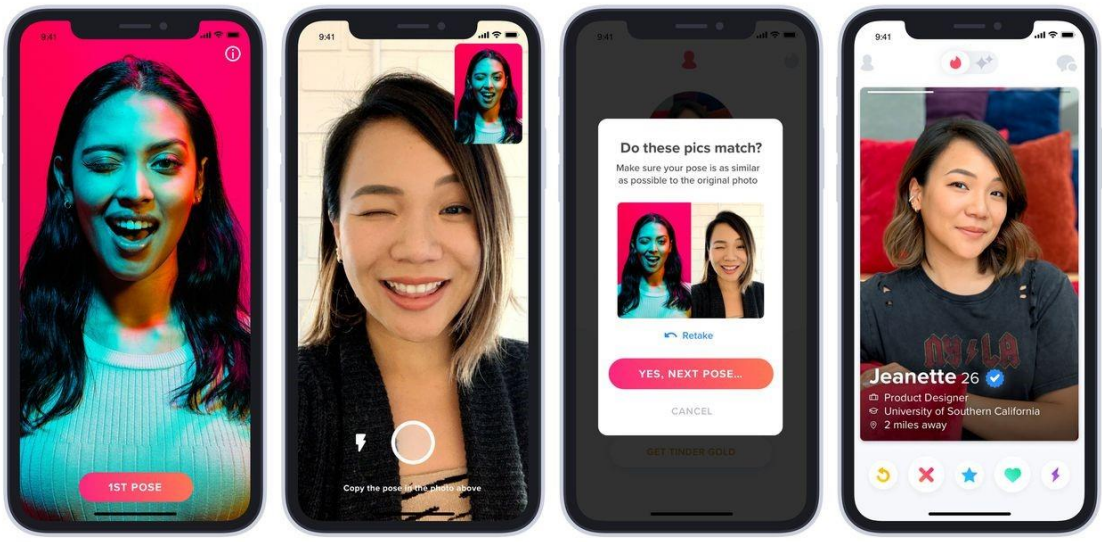
This method will delegate the verification process on those platforms instead assuming that you won’t be able to create an anonymous Google/Facebook/Apple/Twitter account with ease.

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 won’t cover this one (yet) as it’s mainly used on financial platforms (that will be able to identify you with other means anyway) and some dating apps like Tinder[201]. Unfortunately this method is now also sometimes being used on Facebook[202] and Instagram as part of their verification methods (tho I didn’t face it yet so far).

In some cases these verifications have to be done from your Smartphone and with an “in-app” camera to prevent you from sending a previously saved (edited) image.

This verification is very hard to defeat but not impossible. 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 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).

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’s real or not based on their opinion.

Pros: Usually that verdict is “final” and you’ll probably avoid further issues if you’re good.

Cons: Usually that verdict is “final” and you’ll probably be banned without any appeal possibility if you’re not good.

Getting Online:

Now that you have an understanding of all the ways you can be de-anonymized, tracked and verified. Let’s get started at evading these while remaining anonymous. Remember:

- You can’t trust ISPs
- You can’t trust VPS providers
- You can’t trust public Wi-Fi providers
- You can’t trust Mobile Network providers
- You can’t trust VPN providers
- You can’t trust any Online Platform
- You can’t trust Tor
- You can’t trust your Operating systems (especially Android and Windows).
- You can’t trust your Laptop
- You can’t trust your Smartphone (especially Android).
- You can’t trust your Smart devices
- You cannot trust people.

Basically trust no one and nothing (oh yeah that’s easy).

Do not start this process unless:

- **You consulted your local law for compliance and the legality of your actions.**
- **You are in a safe place with a public Wi-Fi without your smartphone or any other smart device on you.**
- **You are fully done and preparing one of the routes:**
    - **You are running TAILS**
    - **You are running a Whonix Workstation VM.**
    - **You are running a Windows VM with traffic routed through Whonix Gateway.**
    - **You are running a VM within Qubes.**

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 depends on the anonymity of your phone number and the burner phone. If your phone number is not anonymous and your burner phone can be traced back to you, you can be de-anonymized.

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”.

I will help you bit by listing a few tips I learned while doing research over the years:

- Some animals are more equal than others.
    - Ethnicity is important and you will have less issues and attract less attention to verification algorithms if you're Caucasian/East-Asian than if you're Arabic/Black.
    - Age is important and you will have less issues if you're young (18-22) than if you're middle-aged or old.
    - Sex/Gender is important and you'll have fewer issues if you're a female than if you're a male.
    - Country of origin is important and you'll have fewer issues if your identity is Norwegian than if it's Ukrainian or Mexican.
    - Country of residence is important and you'll 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'll have fewer issues if you speak proper English or the language of your Identity than if you use a non-related language. Don't make a Norwegian born Caucasian 20 year old female that speaks Ukrainian or Arabic.
- Similarly, Identities that are "EU residents" with an "EU IP" (VPN/Tor) will benefit from GDPR protections on many platforms. Others will not. GDPR is your friend.
- 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). You should exclude any exit IP that is not located in Western Europe/North America/Japan/South Korea/Australia (excluding Mexico) as you will have less issues with those. 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 have less issues with captchas and online platforms[199] 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/ 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. 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 don't have an "easy way" of doing that yet.
- Create in advance and store in KeePassXC each identity details that should include:
    - Date of Birth
    - Country of Birth
    - Nationality
    - Country of Residence
    - Address of Residence
    - Languages spoken
    - Occupation (Job Title, University, …)
    - Some Interests
    - Phone number (this is your pre-paid SIM card phone number on your Burner phone)
- Do not pick an occupation at a well-known private corporations/company as they have people in their HR depts monitoring activities in platforms such as LinkedIn and will report your profile as being fake if it doesn't match their database. Instead pick an occupation as a freelancer or at a large public institution where you'll face less scrutiny.
- Keep track (write down) of the background stories of your Identity. 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 as the Ministry of Health one day and later on another platform say you work as an intern at the Ministry of Transportation, people will question your identity.

- 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.
- **Consider using the recommended tools on https://privacytools.io/ for your various purposes instead of the usual mainstream tools.**

Note: If you're 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[203].
- On Tor Browser: Edit the torrc file located at Browser/TorBrowser/Data/Tor[204].

Once you're 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're too restrictive. You can see a visualized list of available Exit Nodes here: https://www.bigdatacloud.com/insights/tor-exit-nodes

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/

Overview:

Service	Against ToS	Require Phone	Require E-Mail	VPN Sign-up	Tor Sign-up	Captchas	ID Verification	Facial verification	Overall difficulty
Discord	No	No	Yes	Yes	Yes	No	No	No	Medium
Facebook	Yes	Yes	Yes	Maybe	Maybe	Yes	Maybe	Maybe	Hard
GitHub	No	No	Yes	Yes	Yes	Yes	No	No	Easy
Google	No	Maybe	Maybe	Yes	Yes	Yes	No	No	Medium
Instagram	Yes	Maybe	Yes	Yes	Yes	Yes	No	Maybe	Medium
LinkedIn	Yes	Yes	Yes	Yes	Yes	Yes	Maybe	Maybe	Hard
Microsoft	Yes	Maybe	Maybe	Yes	Yes	Yes	No	No	Medium
ProtonMail	No	Maybe	Maybe	Yes	Yes	Yes	No	No	Medium
Reddit	No	No	No	Yes	Yes	No	No	No	Easy
Telegram	No	Yes	No	Yes	Yes	No	No	No	Easy
Twitter	No	Maybe	Yes	Yes	Yes	Yes	No	No	Medium
4chan	No	No	No	No	No	Yes	No	No	Hard

Discord:

- Is this against their TOS? No https://discord.com/terms
- Will they require a phone number? No they require an e-mail

- Can you create accounts through Tor? I had no issues with that so far

Steps after creating: Enable 2FA authentication with KeePassXC TOTP

Facebook:

- Is this against their TOS? Yes https://www.facebook.com/terms.php

"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's very difficult and their onion address[205] won't help. In most cases you'll just have a random error at sign-up and your account suspended after sign-in.

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're "lucky" (I assume if you're 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 have to 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're 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's also possible that they ask you to take a selfie video or picture making certain gestures to prove your identity. If that's the case, I'm afraid it's a dead end for now.

If you do file an appeal, you will have to wait for Facebook to review it (I don't 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? No https://docs.github.com/en/free-pro-team@latest/github/site-policy/github-terms-of-service
- 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.

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.

Google:

- Is this against their TOS? No https://policies.google.com/terms
- 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 definitely be required

ProtonMail is good … but to appear less suspicious, it's just better to also have a 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 amount of accounts that can be created during the sign-up[206,207].

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 burner phone and pre-paid SIM card to create the account. Don't 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. Firs you'll have to enable 2FA using the Burner phone > Then you'll 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's done, remove the phone 2FA from the Google account. This will prevent someone from using that phone number in the future (when you don't 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 don't 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.

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 [208] (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[209] 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 won't be able to use it to sign-up on a different account. Be careful.

Instagram:

- Is this against their TOS? Yes https://help.instagram.com/581066165581870?ref=dp

"You can't impersonate others or provide inaccurate information. You don't 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 aren't, and you can't create an account for someone else unless you have their express permission." But this clause of their TOS is illegal in Germany (see beginning of this guide).

- 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 definitely be required

It's no secret that Instagram is part of Facebook however it's more lenient than Facebook when it comes to user verification. It's quite unlikely you'll get suspended or banned after signing-up. But it could help.

It's also possible that they ask you to take a selfie video or picture making certain gestures to prove your identity. If that's the case, I'm afraid it's a dead end for now.

For instance I noticed that you'll 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 won't be able to enable Authenticator 2FA from the web for a reason I don't understand.

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

LinkedIn:

- Is this against their TOS? Yes https://www.linkedin.com/legal/user-agreement

" 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 beginning of this guide).

- 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 definitely 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 corporations 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[210] 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're 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

Microsoft:

- Is this against their TOS? Yes https://www.microsoft.com/en/servicesagreement/

"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 beginning of this guide).

- Will they require a phone number? Maybe but not always. Even on Tor depending on your luck/exit node, it's possible that they will only require e-mail verification.
- Can you create accounts through Tor? Yes you can but expect captchas, e-mail verification at least **and maybe phone verification.**

So yes it's 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.

ProtonMail:

- Is this against their TOS? No https://ProtonMail.com/terms-and-conditions
- Will they require a phone number? Maybe. This depends on the IP you're coming from. If you come from Tor, it's likely. From a VPN, it's 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.

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're recommended by privacytools.io[211]. 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[212]. As long as their claim is true and the hash is not linked to your account, and that you followed my guide regarding the Burner phone and the pre-paid SIM card, you should be safe from tracking.

Create this e-mail account first using the burner phone as verification if necessary.

When you're 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.

Reddit:

- Is this against their TOS? No https://www.redditinc.com/policies
- Will they require a phone number? No they won't.
- Can you create accounts through Tor? Yes

Reddit is simple. All you need to register is a valid username and a password. Normally they don't 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.

Telegram:

- Is this against their TOS? No https://telegram.org/tos
- 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.

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 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

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 a week or so later.
- Can you create accounts through Tor? Yes but expect some captchas and your phone number will definitely be required

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'll have to pick up and actually 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 [213], provide a good reason and wait for the appeal to be processed by Twitter. During that process, it's 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's 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 have to 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. Don't use this account for trolling.

4chan:

- Is this against their TOS? No

- Will they require a phone number? No they won't.
- Can you post there with Tor or VPN? Not likely

4chan is 4chan … This guide won't explain 4chan to you. As far as I know, this guide will be of very little help to you if you intend to post to 4chan anonymously. They block Tor exit nodes and VPN IP ranges. It's very unlikely you'll manage to use any of those to post to 4chan using this guide. But it will help you browse 4chan anonymously.

You're gonna have to find a different way to post there using proxies that are not known by 4chan blocking system.

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.

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 (Youwave[214], Bluestacks[215] or if you have a powerful PC, Android Studio) 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/
- 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.
- (Least recommended and most complicated) Have a burner Smartphone that you will connect to the VM layered network through Tethering/Sharing of the connection through Wifi. I won't detail this here but it's 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's not even possible on IOS as far as I know). By reliable I mean being sure that the smartphone won't 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 won't help you there as this would actually be illegal in most places.

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.

Backup your work (safely and anonymously):

Do not ever upload encrypted file containers with plausible deniability (hidden containers within them) to most cloud services (ICloud, Google Drive, OneDrive, Dropbox). 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 (coming soon).

Covering your tracks:

Make sure you don't keep a copy of this guide anywhere unsafe after. The sole presence of this guide will most likely defeat all your plausible deniability possibilities.

Protecting yourself against forensics:

Tails:

Tails is great, you have nothing to worry about. Shut it down and it's all gone.

Windows:

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's get rid of any diagnostic data that could still be there:

- After each use of your Windows devices, go into Settings, Privacy, Diagnostic & Feedback, Click Delete.

Then let's 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 shouldn't 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[168]), your network connections, app crash information and various errors. It's 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're 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.

- Brave (in case you didn't 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

External Tool Cleaning:

Then we will download a convenient utility called PrivaZer that will allow you delete various traces in various places. Again you should not use this on the Decoy OS.

This will be used for cleaning many things such as:

- The Windows USN journal which stores plenty of information[216].
- The Windows System Resource Usage Monitor (SRUM)[217].
- Various histories of various programs (such as the recent lists).
- The free (unallocated) space of your hard drive[218].

Here are the steps:

- Download and install PrivaZer from https://privazer.com/en/download.php
    - Run Privazer after install
    - Use the Wizard:
        - Advanced User
        - Yes remove invalid shortcuts
        - Yes empty recycle bin without a trace
        - Yes remove office software histories
        - Yes remote photo/images software histories
        - Yes remove thumbnail cache
        - Yes remote autocomplete history
        - Yes delete thumbnails for websites
        - Yes delete the open pages from my last session
        - Yes automatic selection of cookies
        - Yes remove all webcache
        - No don't remove shellbags (we will use a different software for this).
        - Yes remove MS games histories
        - Yes remove previous installations of Windows
        - Yes clean Windows updates
        - Yes clean Windows Pre-Fetch
        - Yes disable hibernation
        - Push Scan
        - Select 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, Select SSD with Trim[173] + 1 pass zero (just to be sure as mentioned earlier, Trim itself should be enough[176])
            - If you have an HDD drive, Select HDD with at least 1 pass.

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[172] and you need to clean those. Especially if you mounted any "hidden volume" anywhere. Again you shouldn't do this on the Decoy OS.

    - Download Shellbag Analyzer & Cleaner from https://privazer.com/en/download-shellbag-analyzer-shellbag-cleaner.php

- 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 (don't backup)
    - Select SDD cleanup (if you have an SSD)
    - Select 1 pass (All zero)
    - Clean

Wi-Fi History:

Now it's turn 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 so you'll 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
- Within regedit, enter this to the address bar: " Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles "
- There you'll 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.

How to securely wipe your whole laptop if you want to erase everything:

Linux:

Follow these instructions: https://linuxhint.com/completely_wipe_hard_drive_ubuntu/

Windows:

Unfortunately you won't be able to wipe your Host OS using the built-in tools within the settings. This is because your bootloader was modified with Veracrypt and will make the whole thing fail.

Some laptops offer secure erase from the BIOS and you can check this yourself from your BIOS. If it doesn't, you'll have to wipe it using bootable USB key again. But this time not Windows.

There are several utilities that are recommend (like the old unmaintained DBAN[219]) for this but personally, I will recommend the use of ShredOS.

Feel free do go with DBAN instead if you want, the process is basically the same but might not work out of the box with UEFI laptops.

- Download ShredOS from https://github.com/PartialVolume/shredos.2020.02
- Unzip the ISO file
- Download Rufus from https://rufus.ie/
- 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

If you think you got burned:

If you have some time:

- Don't Panic.
- Destroy the SIM card and trash it in a random trash can somewhere.
- Erase then destroy the Burner phone and trash it in a random trashcan somewhere.
- Securely erase the laptop hard drive "How to securely wipe your whole laptop if you want to erase everything:" and then ideally proceed to physically destroy the HDD/Laptop and trash it somewhere.

If you have no time:

- Try to shut down the laptop as soon as possible and hope for the best

Some last OPSEC thoughts:

- Do not ever use biometrics to safeguard your secrets.
- Do not ever travel with those devices if you have to pass border checks and where they could be illegal (especially the US border).
- Do not plug any equipment in that laptop unless you trust it.
- Remember the first rule of fight club and don't talk to anyone about your anonymous activities using your real identity.
- Keep a normal life and don't be weird. If you spend all your online time using Tor to access the internet and have no social network accounts at all … You're already suspicious and attracting unnecessary attention.
- Encrypt everything but don't take it as granted. Remember the 5$ wrench[5] .
- Keep plausible deniability as an option but remember it won't help against the 5$ wrench either[5].
- Never ever leave your laptop unattended/on/unlocked anywhere. Remember the story of Ross Ulbricht and his arrest https://en.wikipedia.org/wiki/Ross_Ulbricht#Silk_Road,_arrest_and_trial
- Don't talk to the police (at least if you're in the US) https://www.youtube.com/watch?v=d-7o9xYp7eE
- 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.

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 Windows Home or Windows Home N
  - 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).
- Don’t use Online Speech Recognition
- Don’t let app use your location
- Don’t 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 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[220], 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 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 in order to not connect Windows 10 to the internet before those settings are applied. You can either download and copy those to the USB key (for transfer onto a Windows 10 fresh installation) or if it's 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/
    - 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/
    - 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 (20H2) Installation Media using this tool and instructions:

https://www.microsoft.com/en-us/software-download/windows10

- 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.
- Proceed

---

[1] Wikipedia, OSINT https://en.wikipedia.org/wiki/Open-source_intelligence
[2] YouTube Internet Historian Playlist, HWNDU https://www.youtube.com/playlist?list=PLna1KTNJu3y09Tu70U6yPn28sekaNhOMY
[3] Wikipedia, 4chan https://en.wikipedia.org/wiki/4chan
[4] This World of Ours, James Mickens https://scholar.harvard.edu/files/mickens/files/thisworldofours.pdf
[5] XKCD, Security https://xkcd.com/538/
[6] Wikipedia, Threat Model https://en.wikipedia.org/wiki/Threat_model
[7] Bellingcat https://www.bellingcat.com/
[8] Wikipedia, Doxing https://en.wikipedia.org/wiki/Doxing
[9] YouTube, Internet Historian, The Bikelock Fugitive of Berkeley https://www.youtube.com/watch?v=muoR8Td44UE
[10] BBC News, Tor Mirror https://www.bbc.com/news/technology-50150981
[11] GitHub, Real World Onion websites https://github.com/alecmuffett/real-world-onion-sites
[12] Wikipedia, IANAL https://en.wikipedia.org/wiki/IANAL
[13] English translation of German Telemedia Act https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2016/02/Telemedia_Act__TMA_.pdf. 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. ".
[14] Wikipedia, Don't be evil https://en.wikipedia.org/wiki/Don%27t_be_evil
[15] Sneak.Berlin , Your computer is not yours https://sneak.berlin/20201112/your-computer-isnt-yours/
[16] Thenextweb, Apple apps on Big Sur bypass firewalls and VPNs — this is terrible https://thenextweb.com/plugged/2020/11/16/apple-apps-on-big-sur-bypass-firewalls-vpns-analysis-macos/
[17] Wikipedia, IP Address, https://en.wikipedia.org/wiki/IP_address
[18] Wikipedia; Data Retention https://en.wikipedia.org/wiki/Data_retention
[19] Wikipedia, VPN https://en.wikipedia.org/wiki/Virtual_private_network
[20] Wikipedia, Tor Anonymity Network https://en.wikipedia.org/wiki/Tor_(anonymity_network)
[21] Wikipedia, DNS https://en.wikipedia.org/wiki/Domain_Name_System
[22] Wikipedia, DNS Blocking https://en.wikipedia.org/wiki/DNS_blocking
[23] CensoredPlanet https://censoredplanet.org/
[24] ArXiv, Characterizing Smart Home IoT Traffic in the Wild https://arxiv.org/pdf/2001.08288.pdf
[25] Labzilla.io, Your Smart TV is probably ignoring your PiHole https://labzilla.io/blog/force-dns-pihole
[26] Wikipedia, DNS over HTTPS: https://en.wikipedia.org/wiki/DNS_over_HTTPS
[27] Wikipedia, DNS over TLS, https://en.wikipedia.org/wiki/DNS_over_TLS
[28] Wikipedia, Pi-Hole https://en.wikipedia.org/wiki/Pi-hole
[29] Wikipedia, SNI https://en.wikipedia.org/wiki/Server_Name_Indication
[30] Wikipedia, eSNI https://en.wikipedia.org/wiki/Server_Name_Indication#Encrypted_Client_Hello
[31] 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/
[32] 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/

[33] KUL, Encrypted DNS=⇒Privacy?A Traffic Analysis Perspective https://www.esat.kuleuven.be/cosic/publications/article-3153.pdf
[34] ResearhGate, Oblivious DNS: Practical Privacy for DNS Queries https://www.researchgate.net/publication/332893422_Oblivious_DNS_Practical_Privacy_for_DNS_Queries
[35] Nymity.ch, The Effect of DNS on Tor's Anonymity https://nymity.ch/tor-dns/
[36] Wikipedia, IMEI https://en.wikipedia.org/wiki/International_Mobile_Equipment_Identity
[37] Wikipedia, IMSI https://en.wikipedia.org/wiki/International_mobile_subscriber_identity
[38] Android Documentation, Device Identifiers https://source.android.com/devices/tech/config/device-identifiers
[39] Google Privacy Policy, Look for IMEI https://policies.google.com/privacy/embedded?hl=en-US
[40] Wikipedia, IMEI and the Law https://en.wikipedia.org/wiki/International_Mobile_Equipment_Identity#IMEI_and_the_law
[41] Bellingcat,
The GRU Globetrotters: Mission London https://www.bellingcat.com/news/uk-and-europe/2019/06/28/the-gru-globetrotters-mission-london/
[42] 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/
[43] Wikipedia, CCTV https://en.wikipedia.org/wiki/Closed-circuit_television
[44] Apple, Transparency Report, Device Requests https://www.apple.com/legal/transparency/device-requests.html
[45] The Incercept, How Cops Can Secretly Track Your Phone https://theintercept.com/2020/07/31/protests-surveillance-stingrays-dirtboxes-phone-tracking/
[46] Wikipedia, IMSI Catcher https://en.wikipedia.org/wiki/IMSI-catcher
[47] Wikipedia, Stingray https://en.wikipedia.org/wiki/Stingray_phone_tracker
[48] 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
[49] Wikipedia, MITM https://en.wikipedia.org/wiki/Man-in-the-middle_attack
[50] Wikipedia, Faraday Cage, https://en.wikipedia.org/wiki/Faraday_cage
[51] 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
[52] Wikipedia, MAC Address https://en.wikipedia.org/wiki/MAC_address
[53] ResearchGate, Tracking Anonymized Bluetooth Devices https://www.researchgate.net/publication/334590931_Tracking_Anonymized_Bluetooth_Devices/fulltext/5d3308db92851cd04675a469/Tracking-Anonymized-Bluetooth-Devices.pdf
[54] Apple, Differential Privacy White Paper https://www.apple.com/privacy/docs/Differential_Privacy_Overview.pdf
[55] Wikipedia, Differential Privacy https://en.wikipedia.org/wiki/Differential_privacy
[56] Google Android Help, Android Location Services https://support.google.com/accounts/answer/3467281?hl=en
[57] Apple Support, Location Services and Privacy https://support.apple.com/en-us/HT207056
[58] Using Metadata to find Paul Revere (https://kieranhealy.org/blog/archives/2013/06/09/using-metadata-to-find-paul-revere/)
[59] Wikipedia, Google SensorVault, https://en.wikipedia.org/wiki/Sensorvault
[60] 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/
[61] New York Times https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html
[62] 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/
[63] Wikipedia, Geofence Warrant https://en.wikipedia.org/wiki/Geo-fence_warrant
[64] Wikipedia, Room 641A https://en.wikipedia.org/wiki/Room_641A
[65] Wikipedia, Edward Snowden https://en.wikipedia.org/wiki/Edward_Snowden
[66] Wikipedia, Permanent Record https://en.wikipedia.org/wiki/Permanent_Record_(autobiography)
[67] Wikipedia, XKEYSCORE https://en.wikipedia.org/wiki/XKeyscore
[68] 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
[69] Wikipedia, MUSCULAR https://en.m.wikipedia.org/wiki/MUSCULAR_(surveillance_program)
[70] Wikipedia, PRISM https://en.wikipedia.org/wiki/PRISM_(surveillance_program)
[71] Justsecurity, General Hayden https://www.justsecurity.org/10318/video-clip-director-nsa-cia-we-kill-people-based-metadata/
[72] Reuters, Exclusive: Apple dropped plan for encrypting backups after FBI complained – sources https://www.reuters.com/article/us-apple-fbi-icloud-exclusive-idUSKBN1ZK1CT
[73] Wired, The Strava Heat Map and the End of Secrets https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/
[74] 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/

[75] 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
[76] 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/
[77] 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
[78] 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/?utm_term=.8514f3a17b1c&itid=lk_interstitial_manual_59
[79] CryptoEngineering, How does Apple (privately) find your offline devices? https://blog.cryptographyengineering.com/2019/06/05/how-does-apple-privately-find-your-offline-devices/
[80] Apple Support https://support.apple.com/en-us/HT210515
[81] 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/
[82] Apple Support, If your Mac is lost or stolen https://support.apple.com/en-us/HT204756
[83] Wikipedia, BLE https://en.wikipedia.org/wiki/Bluetooth_Low_Energy
[84] 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/
[85] Wikipedia, RFID https://en.wikipedia.org/wiki/Radio-frequency_identification
[86] Wikipedia, NFC https://en.wikipedia.org/wiki/Near-field_communication
[87] Samsonite Online Shop, RFID accessories, https://shop.samsonite.com/accessories/rfid-accessories/
[88] Bellingcat, Joseph Mifsud: Rush for the EXIF https://www.bellingcat.com/news/americas/2018/10/26/joseph-mifsud-rush-exif/
[89] HackerFactor Blog, Deanonymizing Tor Circuits https://www.hackerfactor.com/blog/index.php?/archives/868-Deanonymizing-Tor-Circuits.html
[90] KU Leuven, Website Fingerprinting through Deep Learning https://distrinet.cs.kuleuven.be/software/tor-wf-dl/
[91] DailyDot, How Tor helped catch the Harvard bomb threat suspect https://www.dailydot.com/unclick/tor-harvard-bomb-suspect/
[92] 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/
[93] 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/
[94] ResearchGate, The potential harms of the Tor anonymity network cluster disproportionately in free countries https://www.pnas.org/content/early/2020/11/24/2011893117
[95] arXiv, An Analysis of Anonymity in the Bitcoin System https://arxiv.org/abs/1107.4524
[96] 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/
[97] Wikipedia, KYC https://en.wikipedia.org/wiki/Know_your_customer
[98] YouTube, Breaking Monero https://www.youtube.com/watch?v=WOyC6OB6ezA&list=PLsSYUeVwrHBnAUre2G_LYDsdo-tD0ov-y
[99] Monero, Monero vs Princeton Researchers, https://monero.org/monero-vs-princeton-researchers/
[100] ArXiv, Tracking Mixed Bitcoins, https://arxiv.org/abs/2009.14007
[101] Wikipedia, Exploit https://en.wikipedia.org/wiki/Exploit_(computer_security)
[102] Wikipedia, Freedom Hosting https://en.wikipedia.org/wiki/Freedom_Hosting
[103] Wired, 2013 FBI Admits It Controlled Tor Servers Behind Mass Malware Attack https://www.wired.com/2013/09/freedom-hosting-fbi/
[104] Wikipedia, Sandbox https://en.wikipedia.org/wiki/Sandbox_(computer_security)
[105] Wikipedia, CPU https://en.wikipedia.org/wiki/Central_processing_unit
[106] Wikipedia, Intel Management Engine https://en.wikipedia.org/wiki/Intel_Management_Engine
[107] Wikipedia, AMD Platform Security Processor https://en.wikipedia.org/wiki/AMD_Platform_Security_Processor
[108] Wikipedia, IME, Security Vulnerabilities https://en.wikipedia.org/wiki/Intel_Management_Engine#Security_vulnerabilities
[109] Wikipedia, IME, Assertions that ME is a backdoor
https://en.wikipedia.org/wiki/Intel_Management_Engine#Assertions_that_ME_is_a_backdoor
[110] Wikipedia, IME, Disabling the ME https://en.wikipedia.org/wiki/Intel_Management_Engine#Disabling_the_ME
[111] Magnet Forensics, Magnet AXIOM https://www.magnetforensics.com/products/magnet-axiom/cloud/
[112] Cellebrite, Unlock cloud-based evidence to solve the case sooner https://www.cellebrite.com/en/ufed-cloud/
[113] EFF Panopticlick (https://panopticlick.eff.org/)

[114] 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/
[115] 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/
[116] 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
[117] Mozilla Wiki, Fingerprinting https://wiki.mozilla.org/Fingerprinting
[118] Facebook Research, Deepface https://research.fb.com/publications/deepface-closing-the-gap-to-human-level-performance-in-face-verification/
[119] 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/
[120] 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
[121] 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/
[122] Brown Institute, Open Source Investigation, https://brown.columbia.edu/open-source-investigation/
[123] 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/
[124] Google Patent, Techniques for emotion detection and content delivery https://patents.google.com/patent/US20150242679
[125] 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
[126] The Conversation https://theconversation.com/shadow-profiles-facebook-knows-about-you-even-if-youre-not-on-facebook-94804
[127] The Verge https://www.theverge.com/2018/4/11/17225482/facebook-shadow-profiles-zuckerberg-congress-data-privacy
[128] ZDNET https://www.zdnet.com/article/anger-mounts-after-facebooks-shadow-profiles-leak-in-bug/
[129] CNET https://www.cnet.com/news/shadow-profiles-facebook-has-information-you-didnt-hand-over/
[130] Anyvision https://www.anyvision.co/
[131] BBC, Met police deploy live facial recognition technology https://www.theguardian.com/uk-news/2020/feb/11/met-police-deploy-live-facial-recognition-technology
[132] YouTube, The Economist, China: facial recognition and state control | The Economist
https://www.youtube.com/watch?v=lH2gMNrUuEY
[133] 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/
[134] IMDB, Gattaca 1997, https://www.imdb.com/title/tt0119177/
[135] IMDB, Person of Interest 2011 https://www.imdb.com/title/tt1839578
[136] IMDB, Minority Report 2002, https://www.imdb.com/title/tt0181689
[137] Joseph Steinberg, How To Prevent Facial Recognition Technology From Identifying You https://josephsteinberg.com/how-to-prevent-facial-recognition-technology-from-identifying-you/
[138] NIST, Face recognition accuracy with masks using pre-COVID-19 algorithms
https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8311.pdf
[139] Wikipedia, Phishing https://en.wikipedia.org/wiki/Phishing
[140] Grayshirt, https://www.grayshift.com/
[141] Wikipedia, Gag Order, https://en.wikipedia.org/wiki/Gag_order
[142] Wikipedia, National Security Letter https://en.wikipedia.org/wiki/National_security_letter
[143] Heise Online (German), https://www.heise.de/news/Gericht-zwingt-Mailprovider-Tutanota-zu-Ueberwachungsfunktion-4972460.html
[144] 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
[145] Internet Archive, Wipeyourdata, "No logs" EarthVPN user arrested after police finds logs https://archive.is/XNuVw#selection-230.0-230.1
[146] Internet Archive, Invisibler, What Everybody Ought to Know About HideMyAss https://archive.is/ag9w4#selection-136.0-136.1
[147] Wikipedia, Lavabit Suspension and Gag order, https://en.wikipedia.org/wiki/Lavabit#Suspension_and_gag_order
[148] Wikipedia, Warrant Canary https://en.wikipedia.org/wiki/Warrant_canary

[149] Washington Post, The intelligence coup of the century https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/
[150] Swissinfo.ch, Second Swiss firm allegedly sold encrypted spying devices https://www.swissinfo.ch/eng/second-swiss-firm-allegedly-sold-encrypted-spying-devices/46186432
[151] Wired, Mind the Gap: This Researcher Steals Data With Noise, Light, and Magnets https://www.wired.com/story/air-gap-researcher-mordechai-guri/
[152] Privacy International, Timeline of SIM Card Registration Laws https://privacyinternational.org/long-read/3018/timeline-sim-card-registration-laws
[153] Wikipedia, TAILS, https://en.wikipedia.org/wiki/Tails_(operating_system)
[154] It's not mandatory because this guide will help you harden your laptop as much as possible to prevent online 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.
[155] XKCD, Password Strength https://xkcd.com/936/
[156] Wired https://www.wired.com/2013/12/better-data-security-nail-polish/
[157] Wikipedia, Virtual Machine https://en.wikipedia.org/wiki/Virtual_machine
[158] Wikipedia, Plausible Deniability https://en.wikipedia.org/wiki/Plausible_deniability
[159] Wikipedia, Key Disclosure Laws https://en.wikipedia.org/wiki/Key_disclosure_law
[160] Wikipedia, Bitlocker https://en.wikipedia.org/wiki/BitLocker
[161] 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-
[162] Wikipedia Veracrypt https://en.wikipedia.org/wiki/VeraCrypt
[163] OSTIF Veracrypt Audit, 2016, https://ostif.org/the-veracrypt-audit-results/
[164] Wikipedia, Evil Maid Attack https://en.wikipedia.org/wiki/Evil_maid_attack
[165] Wikipedia, Cold Boot Attack https://en.wikipedia.org/wiki/Cold_boot_attack
[166] CITP 2008 (https://www.youtube.com/watch?v=JDaicPIgn9U)
[167] Veracrypt Documentation, Unencrypted Data in RAM https://www.veracrypt.fr/en/Unencrypted%20Data%20in%20RAM.html
[168] Veracrypt Documentation, Data Leaks https://www.veracrypt.fr/code/VeraCrypt/plain/doc/html/Data%20Leaks.html
[169] ResearchGate, Defeating Plausible Deniability of VeraCrypt Hidden Operating Systems https://www.researchgate.net/publication/318155607_Defeating_Plausible_Deniability_of_VeraCrypt_Hidden_Operating_Systems
[170] 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
[171] SourceForge, Veracrypt Forum https://sourceforge.net/p/veracrypt/discussion/technical/thread/53f33faf/
[172] SANS, Windows ShellBag Forensics in-depth https://www.sans.org/reading-room/whitepapers/forensics/windows-shellbag-forensics-in-depth-34545
[173] Wikipedia, Trim https://en.wikipedia.org/wiki/Trim_(computing)
[174] Veracrypt Documentation, Trim Operations https://www.veracrypt.fr/en/Trim%20Operation.html
[175] Veracrypt Documentation, Rescue Disk https://www.veracrypt.fr/en/VeraCrypt%20Rescue%20Disk.html
[176] 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
[177] WindowsCentral, Trim Tutorial https://www.windowscentral.com/how-ensure-trim-enabled-windows-10-speed-ssd-performance
[178] Veracrypt Documentation, Trim Operation https://veracrypt.eu/en/docs/trim-operation/
[179] 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
[180] Milan Broz's Blog, TRIM & dm-crypt ... problems? http://asalor.blogspot.com/2011/08/trim-dm-crypt-problems.html
[181] Veracrypt Documentation, Rescue Disk https://www.veracrypt.fr/en/VeraCrypt%20Rescue%20Disk.html
[182] Wikipedia, Virtualbox https://en.wikipedia.org/wiki/VirtualBox
[183] Wikipedia, Whonix https://en.wikipedia.org/wiki/Whonix
[184] Oracle Virtualbox Manual, Snapshots https://docs.oracle.com/en/virtualization/virtualbox/6.0/user/snapshots.html
[185] 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
[186] Wikipedia, TOTP https://en.wikipedia.org/wiki/Time-based_One-time_Password_algorithm
[187] Wikipedia, Multi-Factor Authentication https://en.wikipedia.org/wiki/Multi-factor_authentication
[188] Wikipedia, Captcha https://en.wikipedia.org/wiki/CAPTCHA
[189] Wikipedia, Turing Test https://en.wikipedia.org/wiki/Turing_test
[190] Google reCaptcha https://www.google.com/recaptcha/about/
[191] hCaptcha https://www.hcaptcha.com/

[192] 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
[193] 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/
[194] 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
[195] Google Blog https://security.googleblog.com/2014/12/are-you-robot-introducing-no-captcha.html
[196] Cloudflare Blog, Cloudflare supports Privacy Pass https://blog.cloudflare.com/cloudflare-supports-privacy-pass/
[197] Privacy International,
Timeline of SIM Card Registration Laws https://privacyinternational.org/long-read/3018/timeline-sim-card-registration-laws
[198] Wikipedia, Device Fingerprinting https://en.wikipedia.org/wiki/Device_fingerprint
[199] 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
[200] Wikipedia, Dark Pattern https://en.wikipedia.org/wiki/Dark_pattern
[201] 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
[202] 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#
[203] Whonix Documentation, https://www.whonix.org/wiki/Tor#Edit_Tor_Configuration
[204] Tor Browser Documentation, https://support.torproject.org/tbb/tbb-editing-torrc/
[205] Facebook Onion Website http://facebookcorewwwi.onion
[206] Google Help https://support.google.com/accounts/answer/114129?hl=en
[207] Google Help https://support.google.com/google-ads/answer/7474263?hl=en
[208] Google, Your account is disabled https://support.google.com/accounts/answer/40695
[209] Google, Request to restore the account https://support.google.com/accounts/contact/disabled2
[210] Jumio, ID verification features https://www.jumio.com/features/
[211] Privacytools.io Recommended E-mail Providers https://privacytools.io/providers/email/
[212] ProtonMail Human Verification System https://ProtonMail.com/support/knowledge-base/human-verification/
[213] Twitter Appeal Form https://help.twitter.com/forms/general
[214] Youwave, https://youwave.com/
[215] Bluestacks, https://www.bluestacks.com/
[216] Medium.com, The Windows USN Journal https://medium.com/velociraptor-ir/the-windows-usn-journal-f0c55c9010e
[217] Medium.com, Digging into the System Resource Usage Monitor (SRUM) https://medium.com/velociraptor-ir/digging-into-the-system-resource-usage-monitor-srum-afbadb1a375
[218] SANS, Timestamped Registry & NTFS Artifacts from Unallocated Space https://www.sans.org/blog/timestamped-registry-ntfs-artifacts-from-unallocated-space/
[219] DBAN, https://dban.org/
[220] Privacytools.io, Operating Systems https://privacytools.io/operating-systems/