**Physical and Hardware Isolation**

Hardware has unique serial numbers that can lead back to the user/buyer

* If the hardware wasn’t bought anonymously

**MAC Address**

This can be taken from your network card

* Was used by the NSA to de-anonymise TOR users through an old Firefox exploit

Ipconfig /all (windows)

Ifconfig (linux/mac)

* Will contain the MAC address of machine

Ip a show eth0

* Will also show hardware address

**HWaddr** 08:00:27:2e:5b:59

* The first 3 bytes are unique to the manufacturer e.g., mac, windows
* The last 3 bytes are specific to the network card, Wi-Fi card, ethernet card etc.
  + Unique to your device

Technitiium.com/tmac has an address changer for windows

MACchanger, available in Kali for Linux

* Not automatically available in Debian
  + Sudo apt-get install -y MACchanger

**To change a MAC address, first you must ‘down’ the network interface**

* + Sudo Ifconfig eth0 down
* When Ifconfig is run again, eth0 won’t be there
* Sudo MACchanger -r
  + -r 🡪 random (change to random MAC address)
* Then bring the interface back up
  + Sudo Ifconfig eth0 up

Wifispoof.com and MacDaddy will also allow you to change your mac address

Generate new MAC address on a VM often to avoid being tied to a specific VM

**Anonymous hardware + MAC changes are the best combination**

**Hardware Serials**

All modern **CPUs** should not have a software readable serial number

* Can only identify a model, not a unique identifier
* CPUz, I-Nex – on windows shows CPU info
* MacCPUID for mac

**Motherboard**

* Often carry unique identifiers in the SMBIOS memory (system management bios), major OEMs will have these numbers in a data store
* Even when using Tails on a paid OS like a windows laptop, then the hardware ID will be shared so complete anonymity isn’t achieved

**DMI Decoder**

Straight download for windows

Sudo apt-get install -y dmidecode for Linux

(Using Brew) Brew install cavaliercoder/dmidecoder/dmidecode

* Brew will also always check for updates
  + Lshw command shows the hardware serial numbers
  + Sudo apt-get install –y lshw
  + Sudo lshw -class disk
  + “System\_profiler SPSerialATAdatatype” also

**Mitigation**

How to change the hardcoded HW IDs

* VolumeID v2.0 for windows
* Chameleon for Windows

Buy Anonymously, no money trail

Using VMs for isolation and compartmentalisation

* **Have their own physical machine ID** with no traceable connection to the host physical machine ID unless exploited

Use a separate phone

Store files separately on an encrypted USB or Hardrive

Security Tokens

Hardware security modules

Store encryption keys separately

* UbiKey
* NitroKey

Store backups off-line for physical isolation

Network Isolation

* Separating trusted devices from un-trusted devices using LANs, VLANs, Firewalls etc.

Separate physical location to operate like an internet café for different aliases