Tails – The Amnesic Incognito Live System

- Operating system designed to protect anonymity and privacy.
- Routes all traffic through the TOR network → No leaks.
- Live OS → it boots from a USB or a DVD.
- Amnesic – leaves no traces of usage.
  - Only uses RAM.
  - Never touches other storage space.
- Comes with a number of encryption & privacy tools

Tails

theamnesicincognitolivesystem

Tails – Installation Options

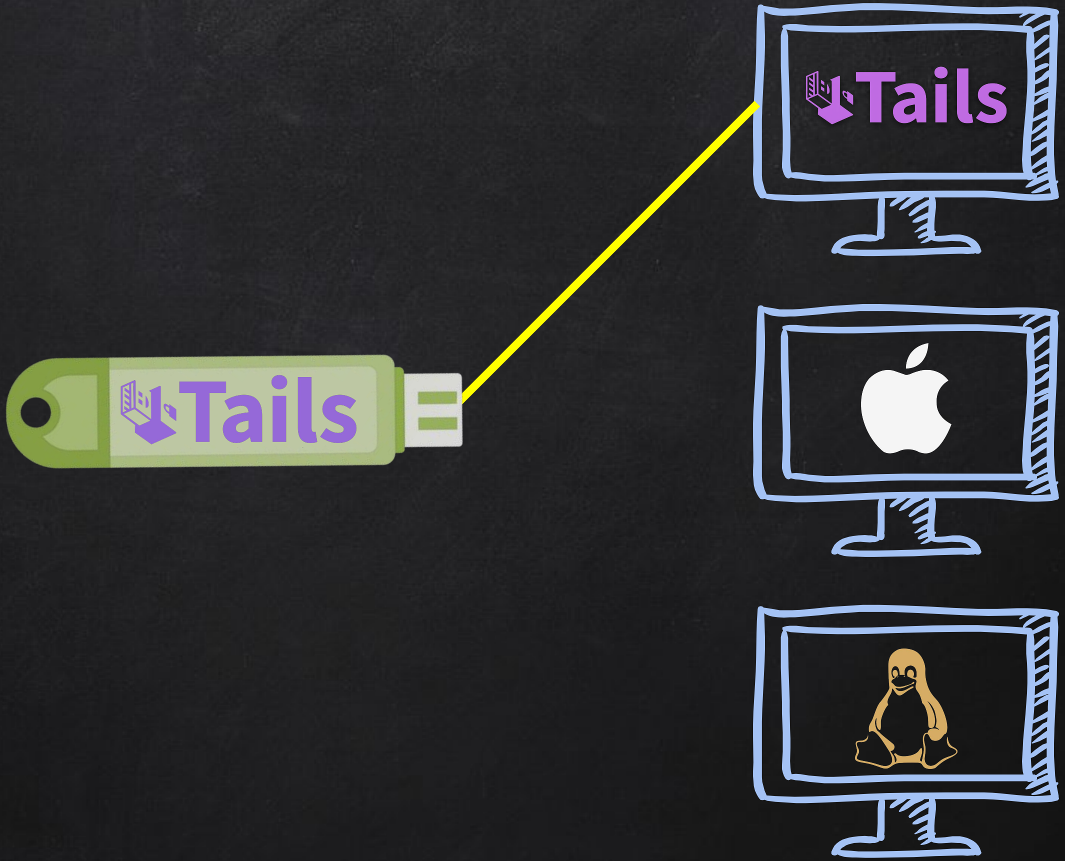
1. As a virtual machine – Loses lots of its benefits:
   - Not fully live.
   - Will leave traces.
   - Not as secure as live.
   - Host OS can still leake info.
2. Burn on DVD – None persistent.
3. On USB stick – Supports persistence.

Note: Once installed, tails will work on any computer regardless of what OS it runs by default.

Installing Tails

Installing Tails

Installing Tails



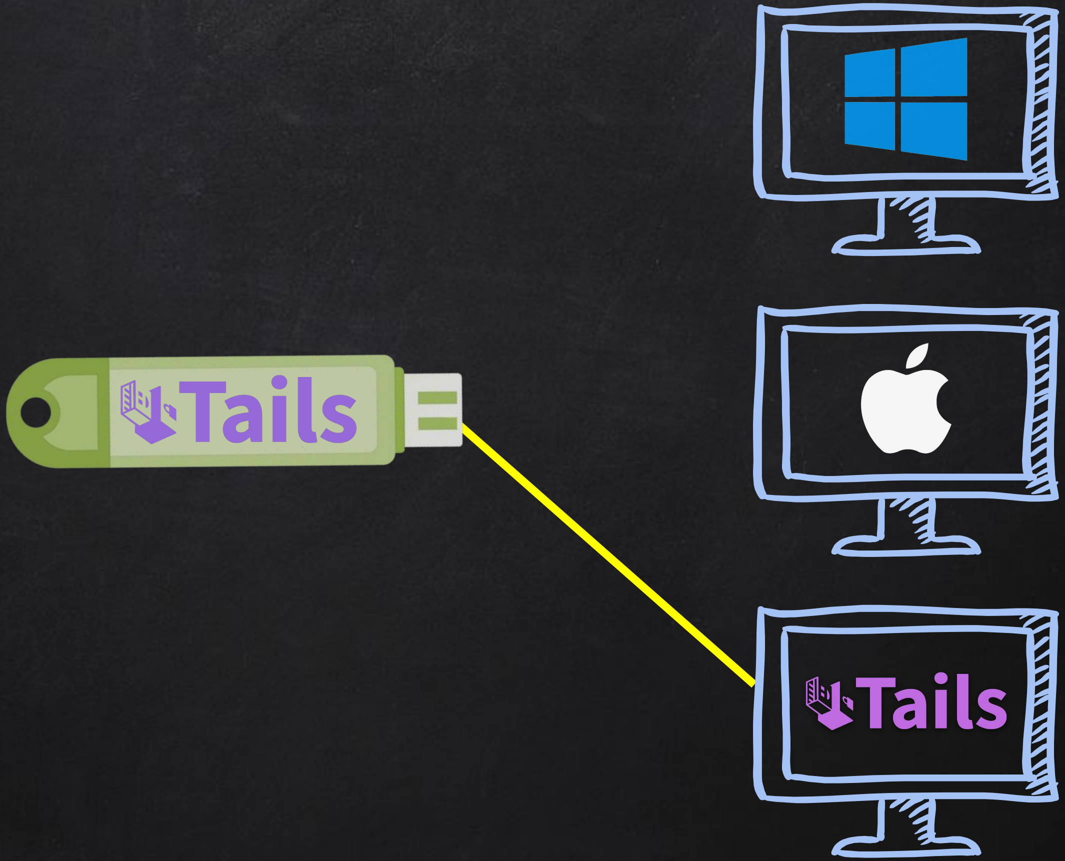
Installing Tails

Installing Tails

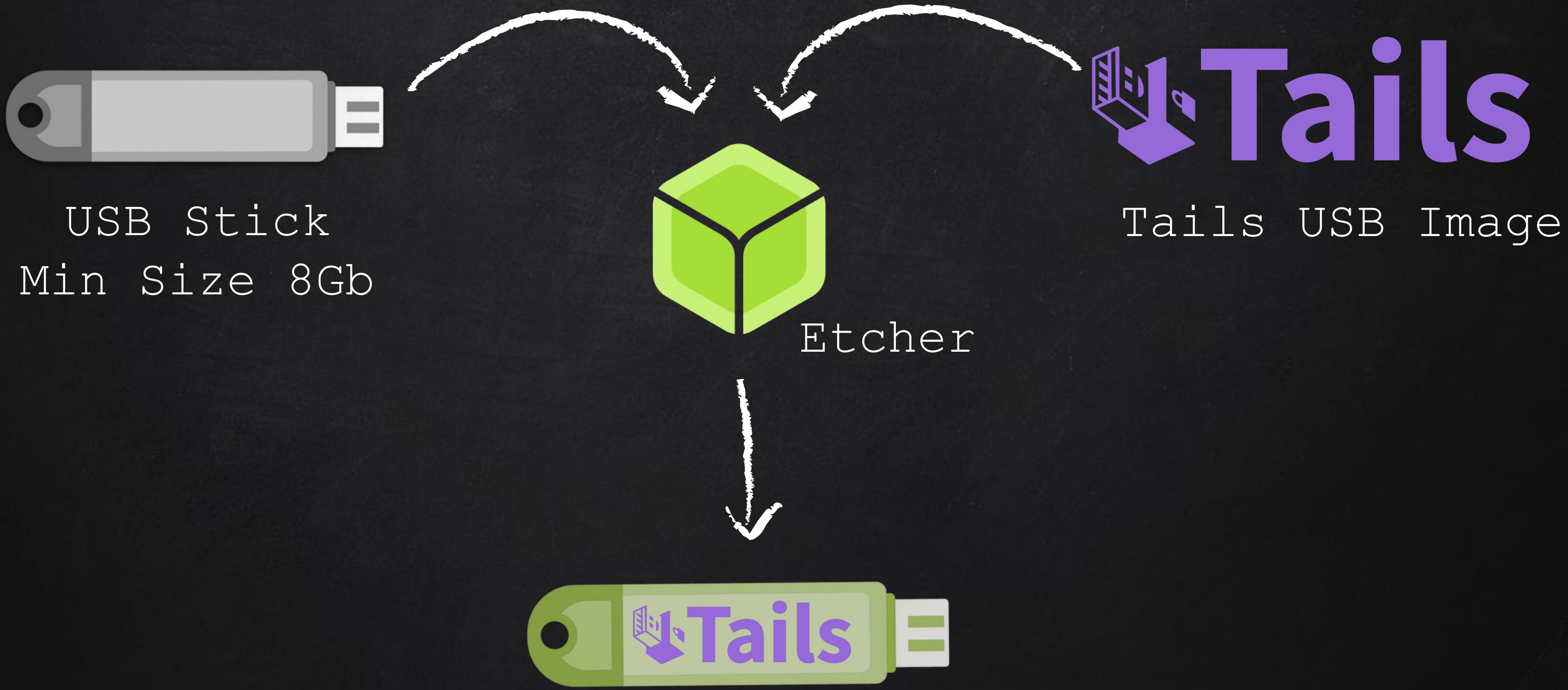
Tails
Tails

Installing Tails

Installing Tails



Installing Tails



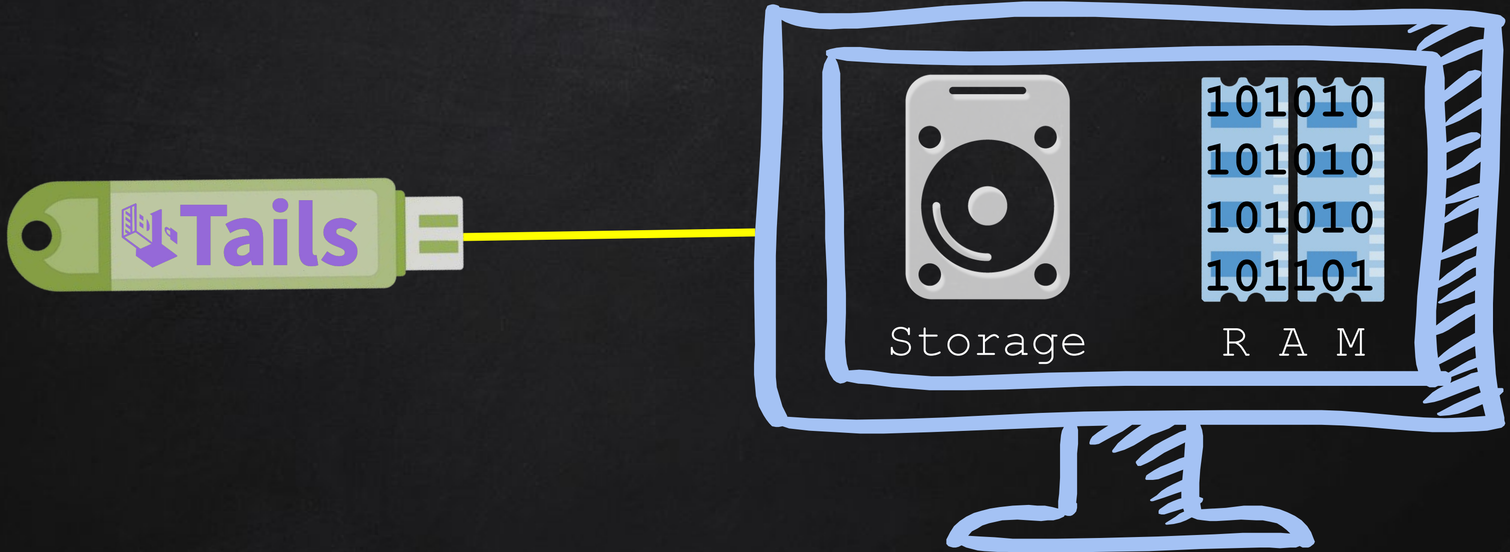
USB Stick
Min Size 8Gb

Etcher

Tails USB Image

Tails – The Amnesic Incognito Live System

- Amnesic – leaves no traces of usage.
  - Only uses RAM.
  - Never touches other storage space.



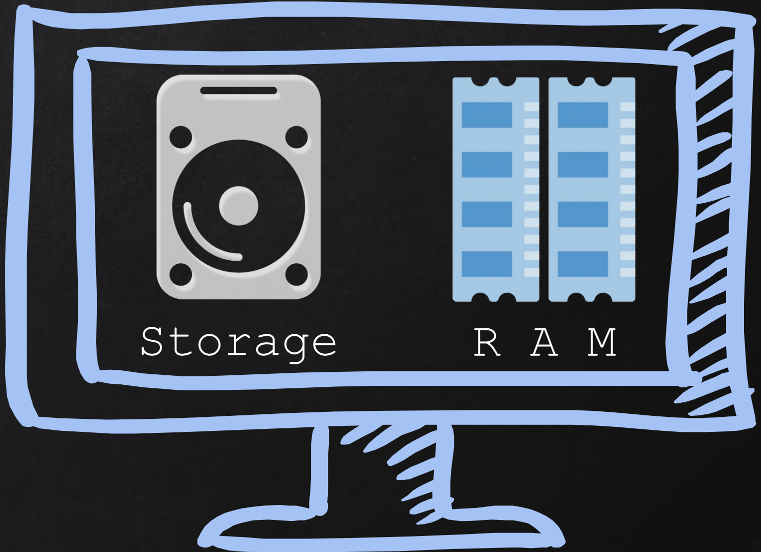
Tails – The Amnesic Incognito Live System

- Amnesic – leaves no traces of usage.
  - Only uses RAM.
  - Never touches other storage space.

Tails
Storage
R A M

Tails – The Amnesic Incognito Live System

- Amnesic – leaves no traces of usage.
  - Only uses RAM.
  - Never touches other storage space.



Starting Tails

1. Connect Tails USB.
2. Start/restart computer.
3. Enter the boot menu.
4. Boot from USB/External storage.

Tails
theamnesicincognitolivesystem

Acer	Esc, F12, F9
Asus	Esc, F8
Dell	F12
Fujitsu	F12, Esc
HP	F9
Lenovo	F12, Novo, F8, F10
Samsung	Esc, F12, F2
Sony	F11, Esc, F10
Toshiba	F12
others…	F12, Esc

Tails – Persistence

- Tails is live and amnesic.
  - Never uses computer storage.
  - Only relies on RAM.

  → Sores nothing forgets everything when shut down.

Benefits – Improved secure, privacy & anonymity.

Disadvantages – Can't store anything.

Tails - Persistence

- Persistence allows us to store files on Tails.
- Computer storage is still left untouched.
- Uses space left on the USB flash drive.
- The persistent volume is encrypted with LUKS with a passphrase of your choice.
- At boot you'll have the choice to unlock the persistent storage.

Tails – Persistence

Benefits

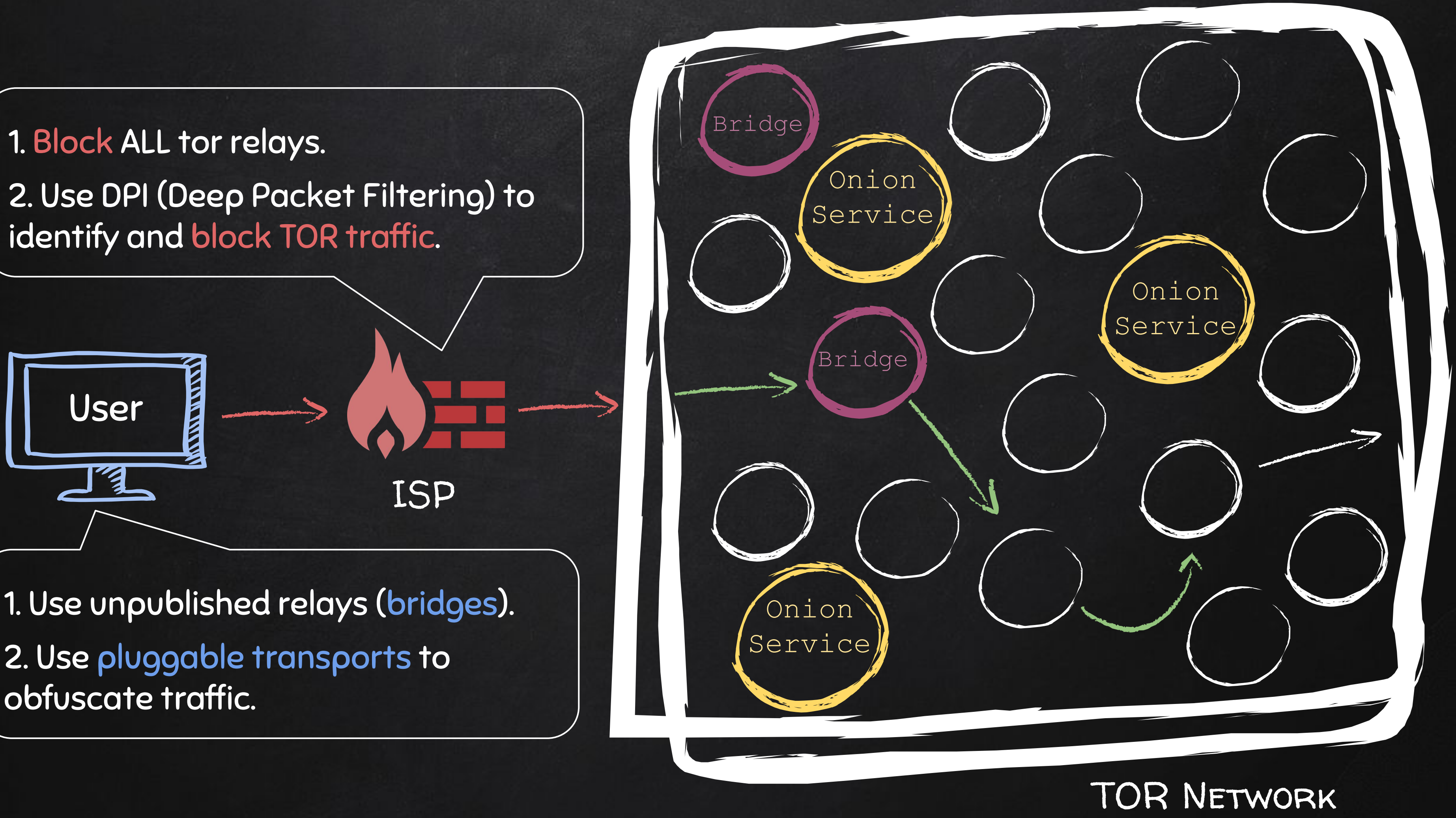
- Best of both worlds!
- Store files, passwords, keys ....etc
- Modify settings.
- Install programs/plugins.

Disadvantages

1. More unique → easier to detect.
2. Incorrect settings or vulnerable software can compromise your anonimity.

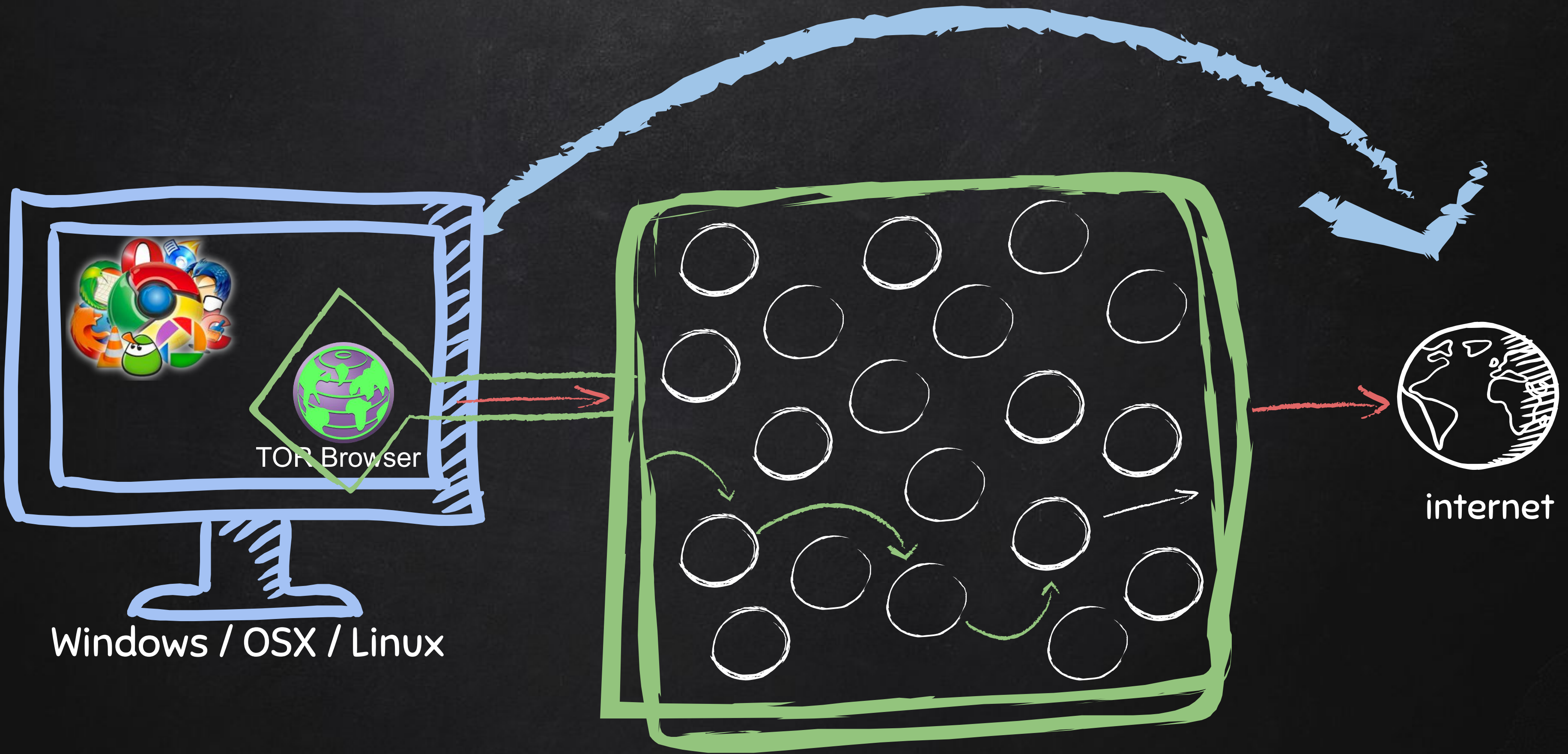
1. Block ALL tor relays.

2. Use DPI (Deep Packet Filtering) to identify and block TOR traffic.



1. Use unpublished relays (bridges).

2. Use pluggable transports to obfuscate traffic.

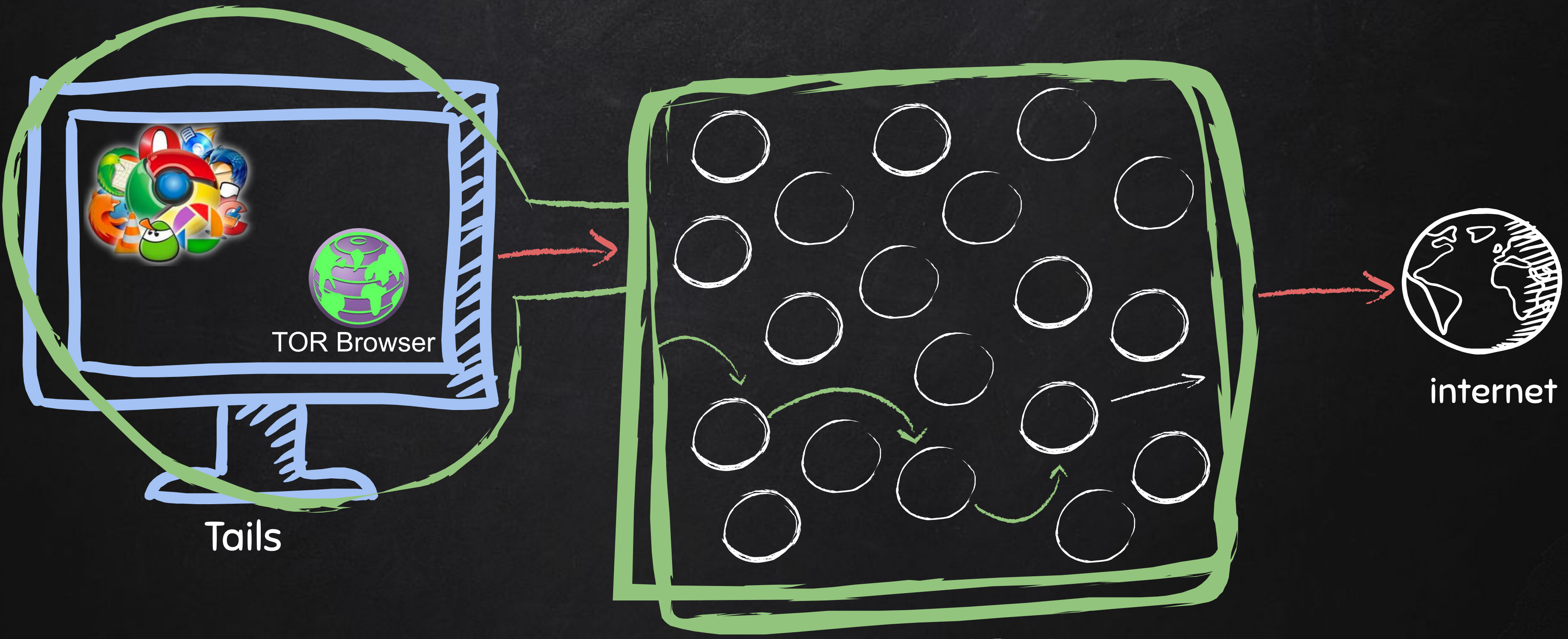


TOR Browser

Windows / OSX / Linux

TOR Network

internet

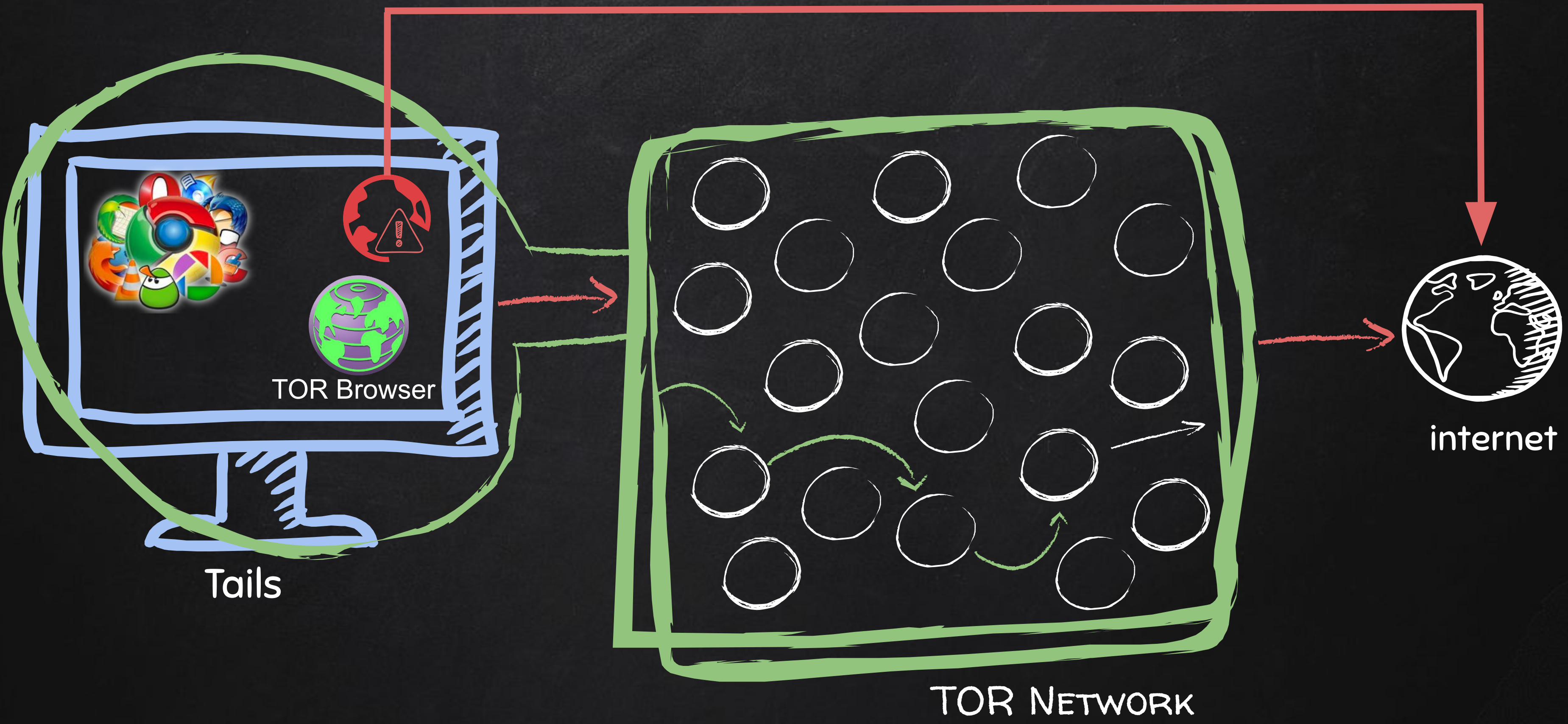


TOR Browser

Tails

TOR Network

internet


TOR Browser
Tails
TOR Network
internet

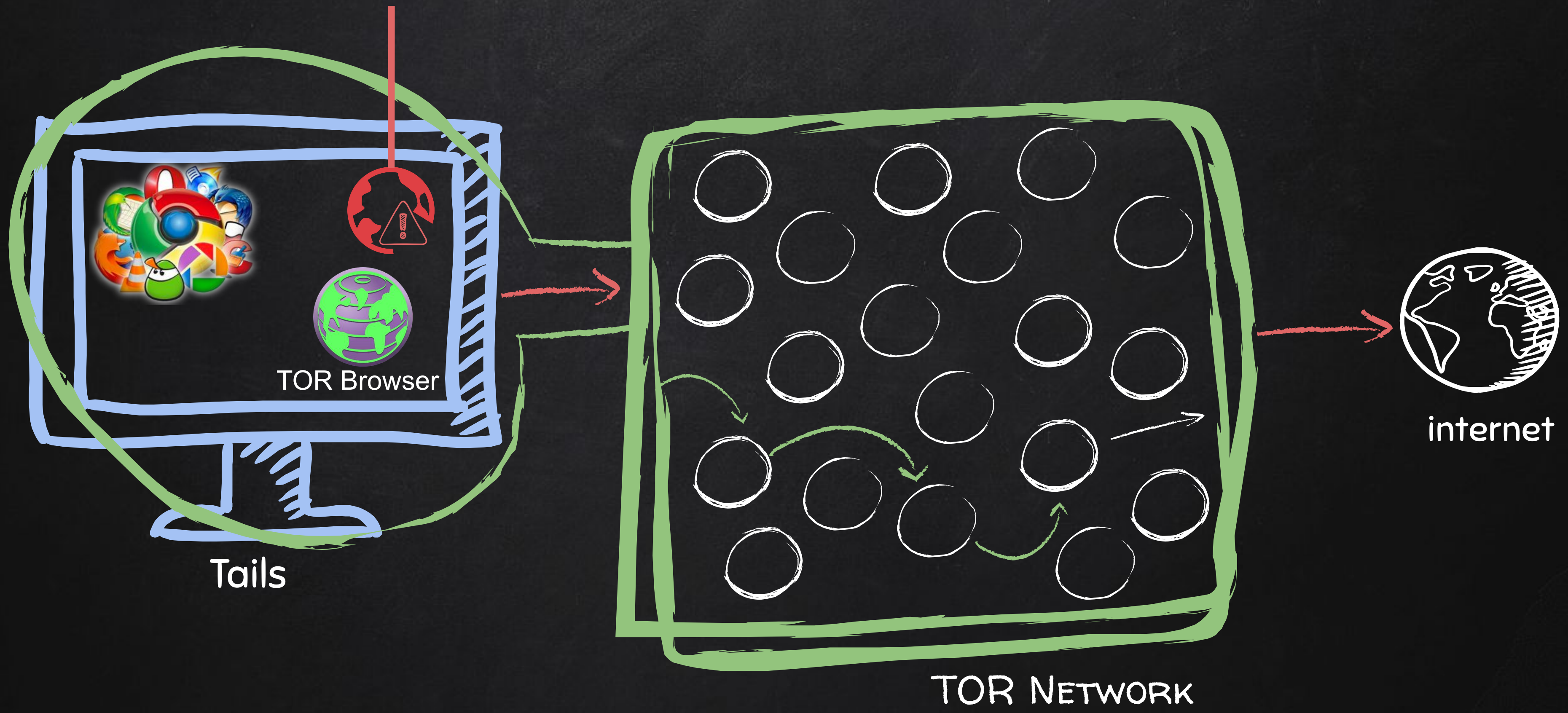
Entry Points - explain .onion sites

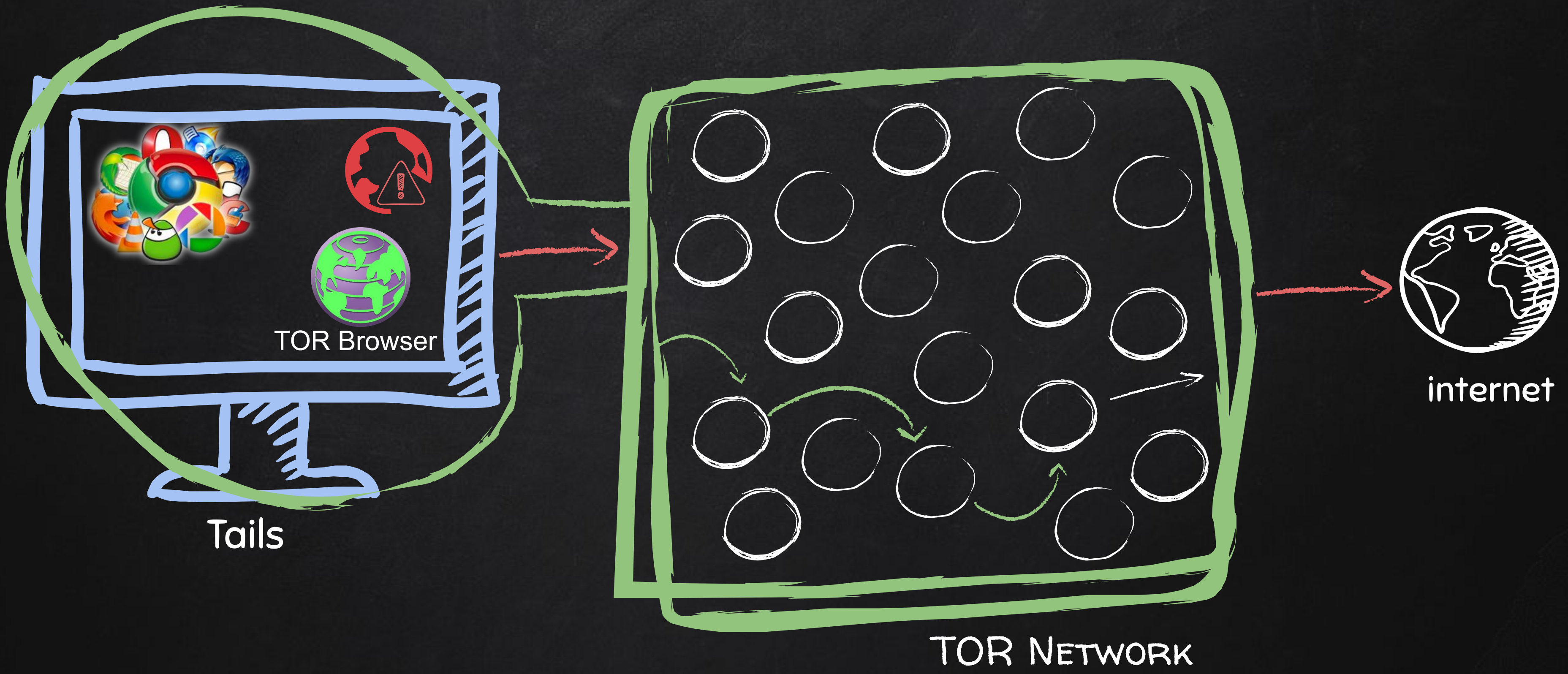
Benefits

- Best of both worlds!
- Store files, passwords, keys ....etc
- Modify settings.
- Install programs/plugins.

Disadvantages

1. More unique → easier to detect.
2. Incorrect settings or vulnerable software can compromise your anonimity.


TOR Browser
Tails
TOR Network
internet


TOR Browser
Tails
TOR Network
internet