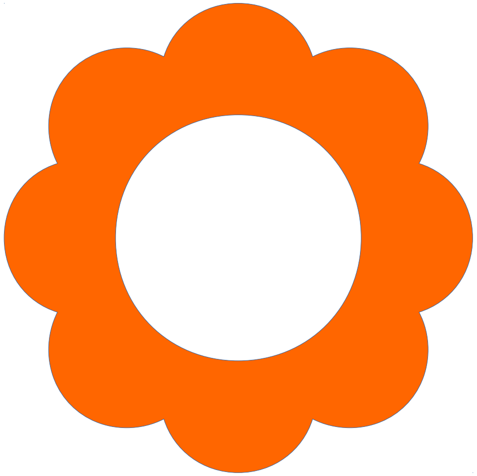
How to live your life while using reasonably secure technologies

Who am I? (Disclaimer)

- A concerned artist
- A free software advocate
- A Vim User
- A lover of the colour orange
- A lover of privacy and freedom
- But still just another student



What do I have to gain?

- Nothing*

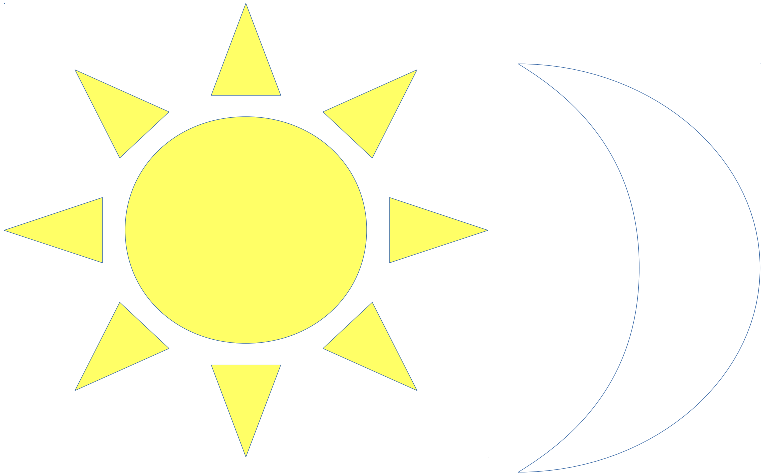
*if there is something let me know

What this talk is

- A discussion that is based around me talking more and you responding when you have questions.
- Not a time to just let me talk fast and you not understand while I stroke my ego and rant about how I hate most tools but not have any better suggestions.
- A chance for me to use all the symbols in impress
- Not super technical unless it wants to be
- An introduction to a few tools

What happened?

- Digital things
- Computers are everywhere and networked
- Very quick development cycles
- Government mass surveillance
- Cheap consumer surveilance technology



This stuff happened in the last week
(Wrote these next slides this morning)

Smart TVs Spying

- WEEPING ANGEL – Fake off mode for targetted surveillance
- http://billmoyers.com/story/dont-say-werent-warned-smart-tv-spying/

Chrome DRM enabled

- “Protected Content” - Allow site to execute code in your browser without you being able to “easily” inspect it.
- http://www.pcworld.com/article/3163235/software/chromes-next-release-will-make-drm-mandatory.html
- https://imgur.com/h5smt2y

Allo shares users search history

- Users of Allo could see fragments of friends search history (fixed now)
- http://www.independent.co.uk/life-style/gadgets-and-tech/news/google-allo-search-history-revealed-messaging-app-a7630001.html

TorrentFreak Fictional story about real law

- https://torrentfreak.com/futureshock-uk-teenager-jailed-for-5-years-for-downloading-one-movie-170312/
- https://services.parliament.uk/bills/2016-17/digitaleconomy.html

Confide doesnt understand the difference between won’t and can’t

- Uploads decryption keys to server
- https://arstechnica.com/security/2017/03/unfixed-weaknesses-in-confide-stoke-doubts-about-end-to-end-crypto-claims/

CIA Leak code going to tech companies

- http://www.reuters.com/article/us-cia-wikileaks-assange-idUSKBN16G27Y

Brainprint passwords

- Use brainwaves to authenticate
- https://phys.org/news/2017-03-brain-unique-ultimate-password.html
- 98% success compared with 99% for fingerprints
- https://ieeexplore.ieee.org/document/4107575/

Telegram hack (fixed)

- Telegram.me was able to be MitM’d, secret messages were not broken

  https://bo0om.ru/telegram-love-phdays-en

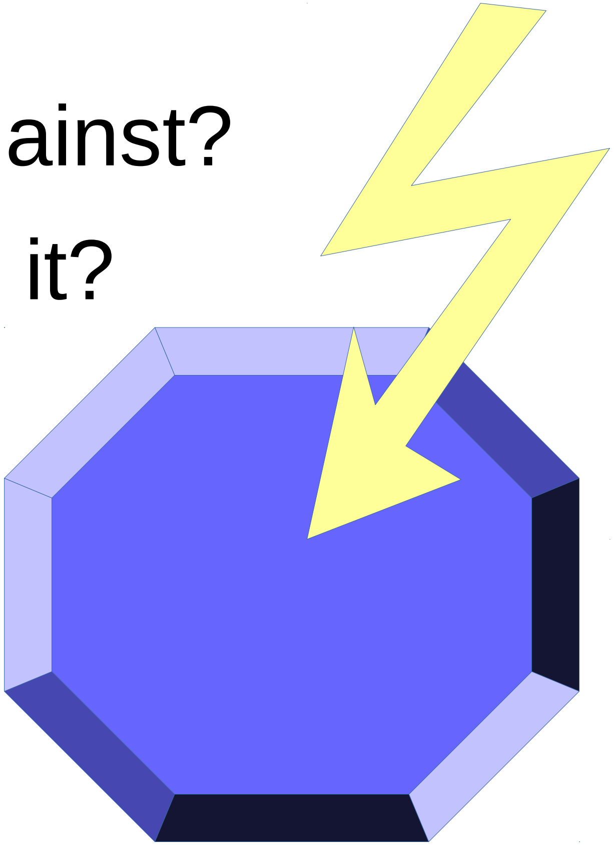
ALWAYS reflash your devices (if you can)

- 2 Companies found preinstalled malware on their devices installed somewhere in transit
- https://arstechnica.com/security/2017/03/preinstalled-malware-targets-android-users-of-two-companies/

Back to the other stuff

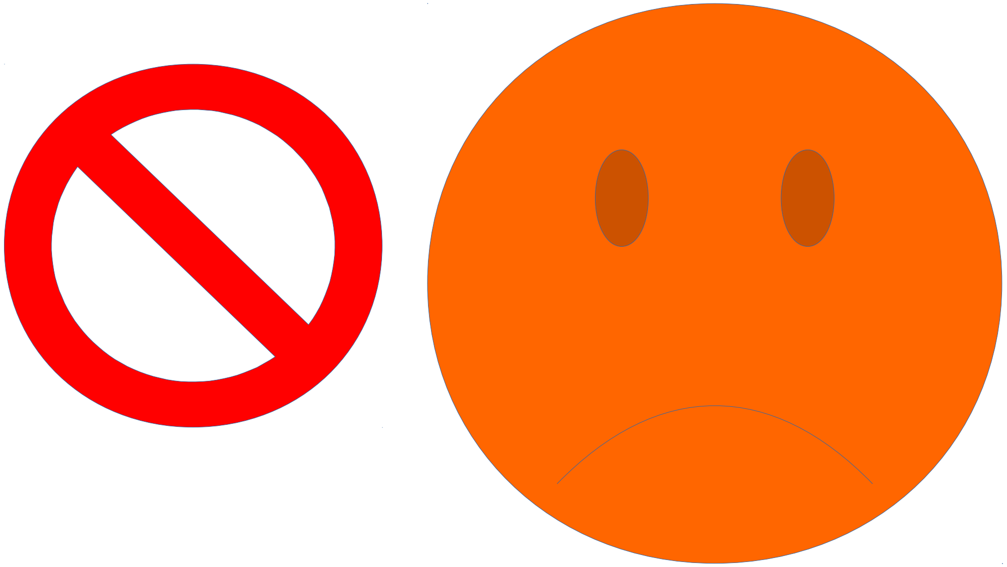
What is a threat model?

- What do I do?
- What do I want to protect?
- Why do I want to protect it?
- Who do I want to protect against?
- How much do I need to use it?



There is no such thing as

- Perfect security*
- Total freedom to compute**
- A best way to communicate privately***

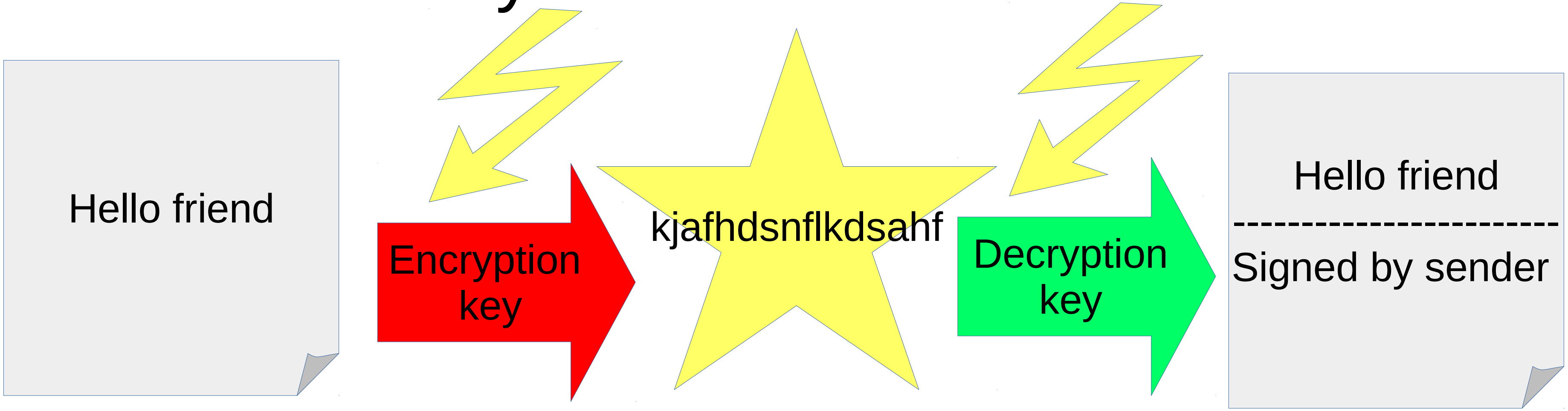


Pareto principle

- AKA 80/20 rule
- What 20% change can give me the 80% improvement

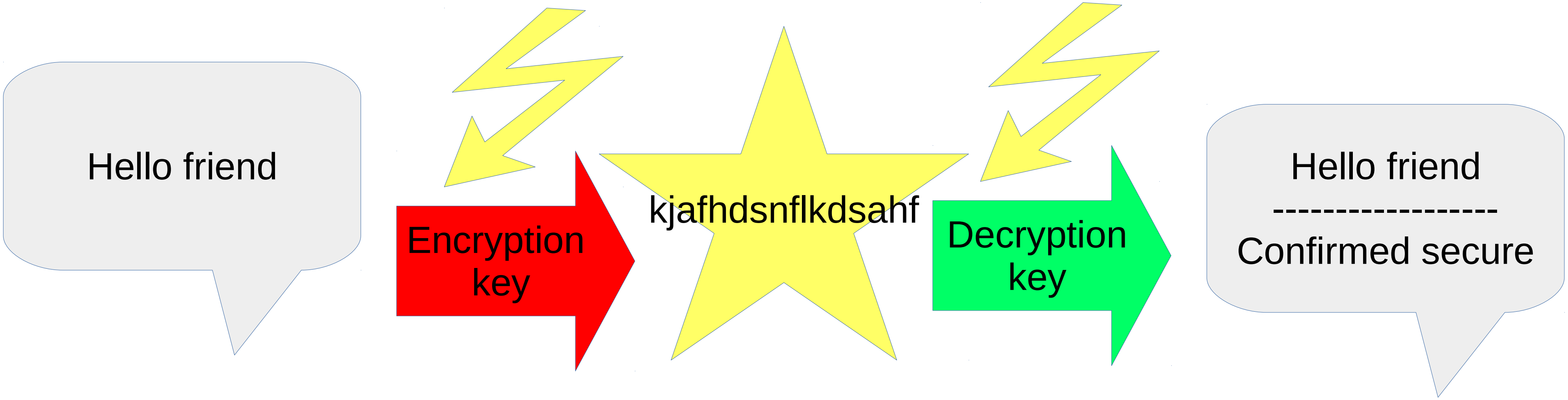
What is GnuPG?

- An implementation of PGP (and others) for encrypting data.
- Could be for Files or messages.
- Tries to tie into the web of trust
- User unfriendly



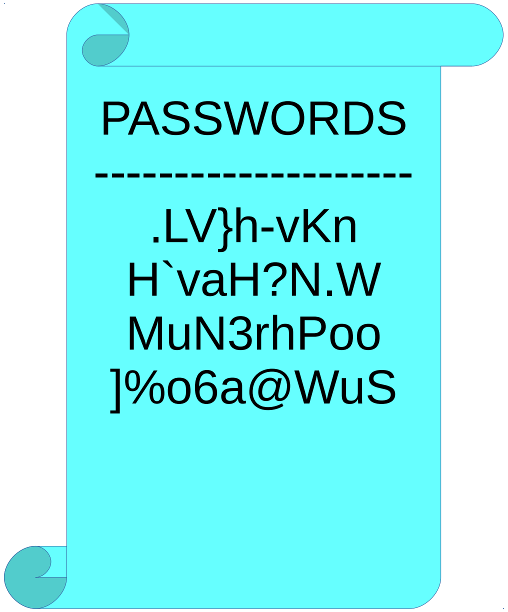
What is Signal?

- A protocol
- Forward secrecy!
- A easy to use instant~ messaging platform
- Not without downsides



What is KeePassX

- Yet another password manager
- Still around from another problem that was solved in the original project but happens to be around everywhere because its compatible and still pretty secure

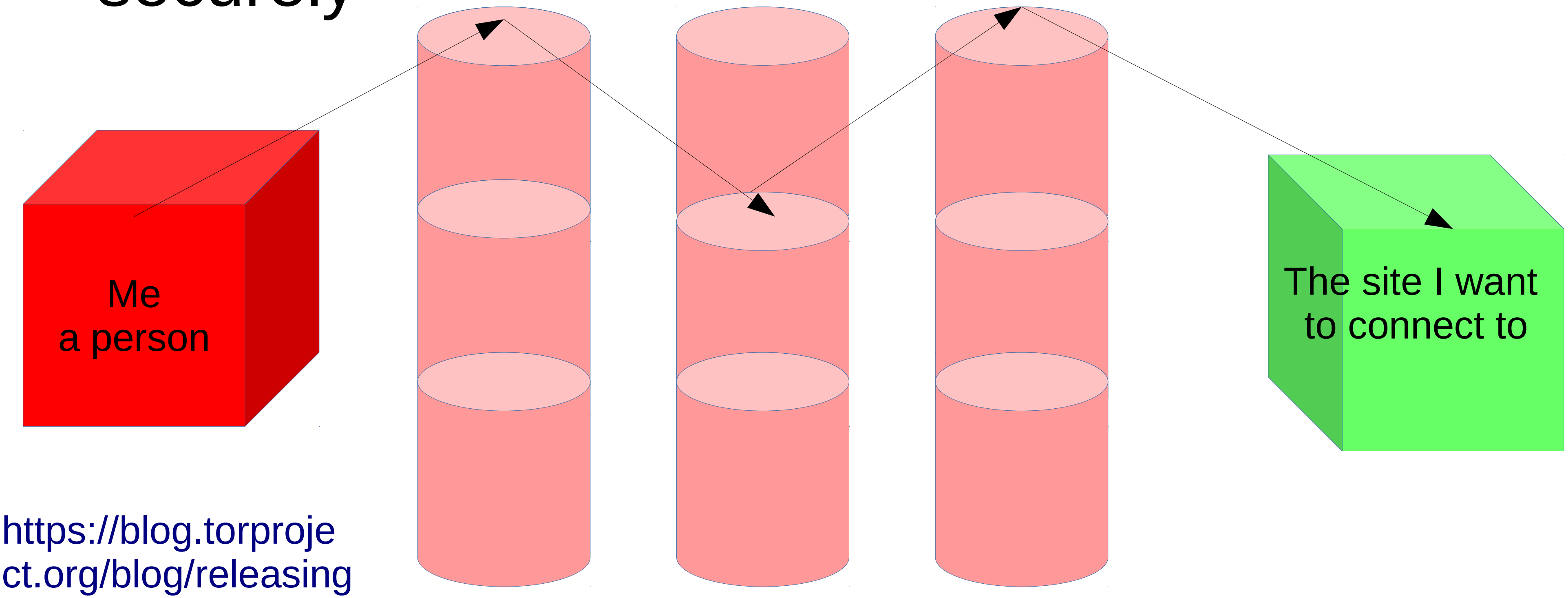


PASSWORDS

.LV}h-vKn
H`vaH?N.W
MuN3rhPoo
]%o6a@WuS

What is Tor?

- A Dark net and traffic anonimizer
- A protocol to have devices communicate securely

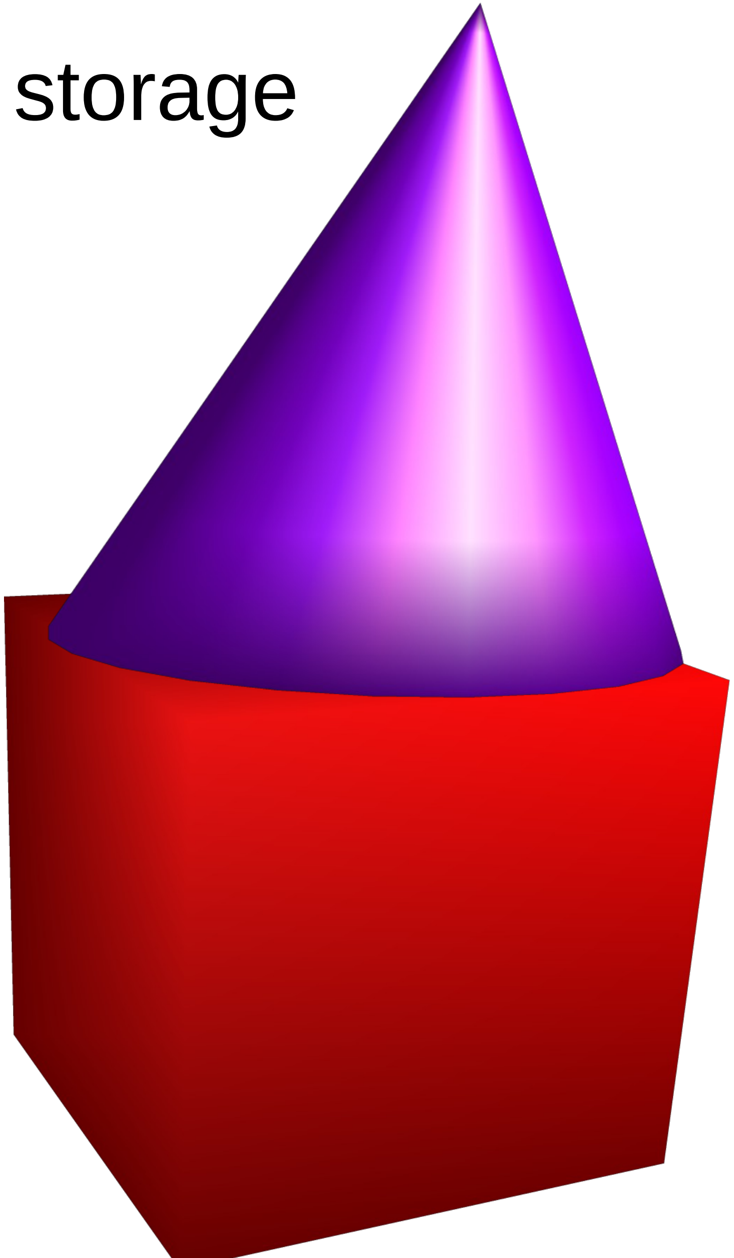


https://blog.torproject.org/blog/releasing-tor-animation

THE TOR NETWORK

What is Tails?

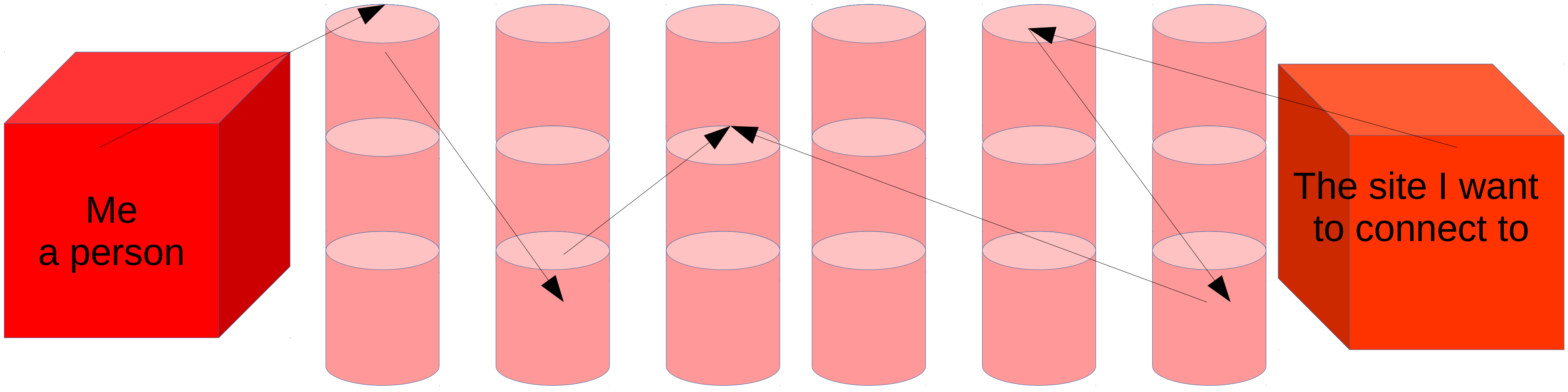
- An Operating system on flash storage
- “Doesnt leave a trace”
- All traffic goes through Tor
- Works on most* computers



https://tails.boum.org/

What is a Tor Hidden/Onion Service

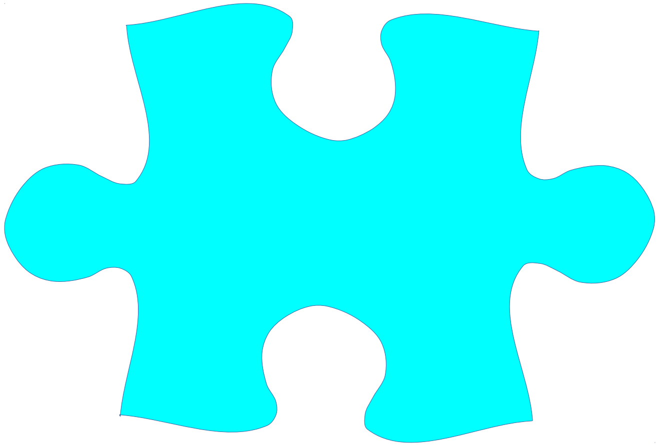
- A site that is accessed through tor but never leaves the network



THE TOR NETWORK

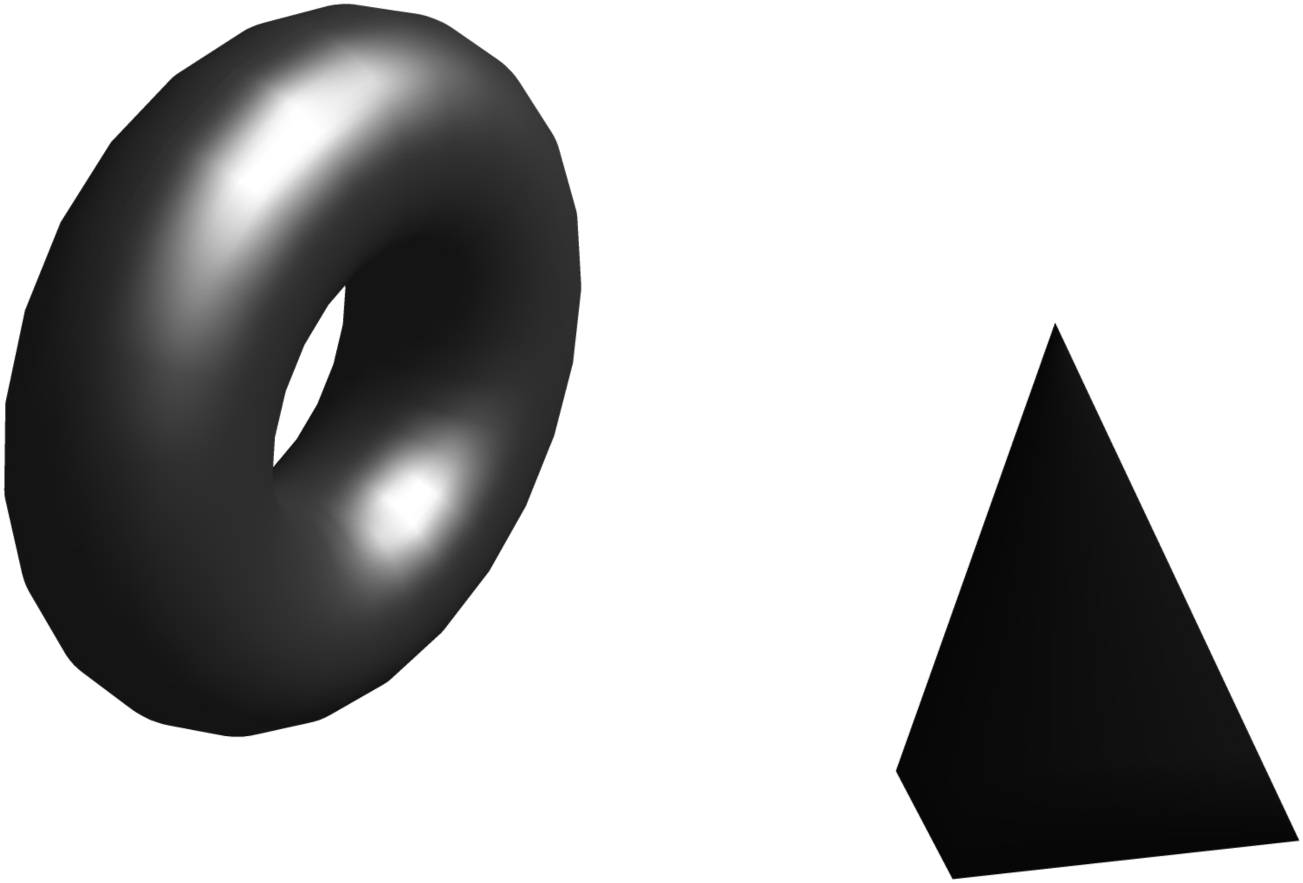
OnionShare / Ricochet

- Ricochet isnt preinstalled.
- OnionShare is.
- Ricochet is an IM, OnionShare is a peer to peer sharing application that works over Tor
- Both use Onion Services



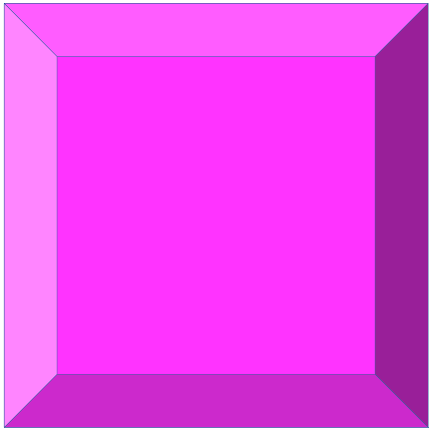
If I didnt demo those things by now

- Stop talking over this slide and demo some things



Raspberry Pi is not secure but...

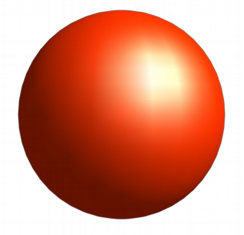
- They aren’t suspicious
- They are kept up to date
- They are easy to find (some are, honest)
- Are reasonably low cost
- CAN be set up easily in most operating systems including Tails (hint hint next slide)



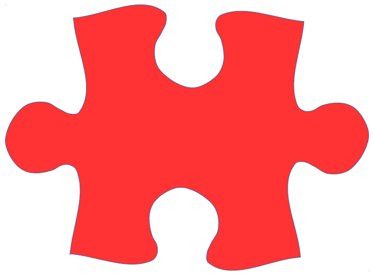
Links to various resources

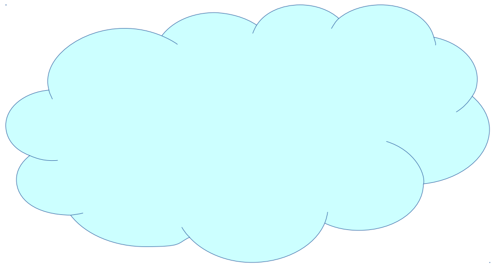
- http://www.teenvogue.com/story/how-to-keep-messages-secure
- https://privacytools.io
- https://prism-break.org/en/
- http://www.tcij.org/sites/default/files/u11/InfoSec%20for%20Journalists%20V1.3.pdf

This is where you spend the rest of time (Bonus Round)



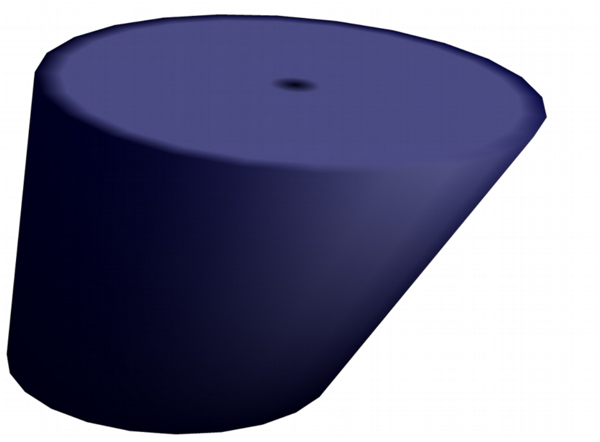
- Set up a Pi Zero W on tails (LIVE)
- Set up eduroam on it (or not if it doesnt work)
- Set up Tor on that Pi Zero W
- Host a website on Tor and serve SSH too!
- Social Media: twitter @_xs github @ixt
- Website: ff4500.red orangeguyrxpij4j.onion (.onion is currently down)
- PGP key fingerprint:
  105C A1F4 AF75 DFE3 04AD C68B 7181 6DF5 3240 20E9





Pi Zero Serial Setup

- Cmdline.txt add after rootwait (modules-load=dwc2,g_cdc)
- Config.txt append (dt-overlay=dwc2)
- After first boot remove and ln
  ln -s lib/systemd/system/getty@.service etc/systemd/system/getty.target.wants/getty@ttyGS0.service



Eduroam on a pi!

- Use wpa_cli
- scan, scan_results, add_network
- set_network n ssid “eduroam”
- set_network n scan_ssid 1
- set_network n proto WPA2
- set_network n priority 1
- set_network n key_mgmt WPA-EAP
- set_network n eap PEAP
- set_network n pairwise ccmp
- identity n username@campus.goldsmiths.ac.uk
- password n password
- set_network n phase2 “auth=MSCHAPV2”
- select_netowork n
- enable_network n
- save_config