CRYPTO.LA

BECOMING ANONYMOUS @ ICP

With Cryptoparty LA

ICE BREAKERS

WHO WE ARE AND WHY WE'RE HERE

Who are you? Why are you here? What are you trying to protect, if anything at all?
And who are you trying to protect it from?

LEVIATHAN

PROGRAM: Icebreaker - Decoder

3⟳: Break up to 3 **code gate** subroutines.

3⟳: +5 strength.

It's efficient as all hell, for certain very large values of "efficient." The whale avatar is either a nice touch or a tragic misapplication of programmer man-hours, depending on who you ask. -BT's Guide to Icebreaking

Illus. Teuku Muharra

3

© 2013 Wizards of the Coast LLC. © 2013 FFG

GS SHRIKE M2

PROGRAM: Icebreaker - Killer - Cloud

If you have at least 2 🔗, the memory cost of GS Shrike M2 is 0, even if it is not installed.

2⟳: Break any number of **sentry** subroutines.

2⟳: +3 strength.

Badder.

Illus. Donald Crank

1

© 2015 Wizards of the Coast LLC. © 2015 FFG

Slowly locking down your data

This workshop will start from small pieces of protection and continue till we understand how to fully lock down our profiles and create alternative identities.

The two main pieces we will cover are:

-browsing

-communication
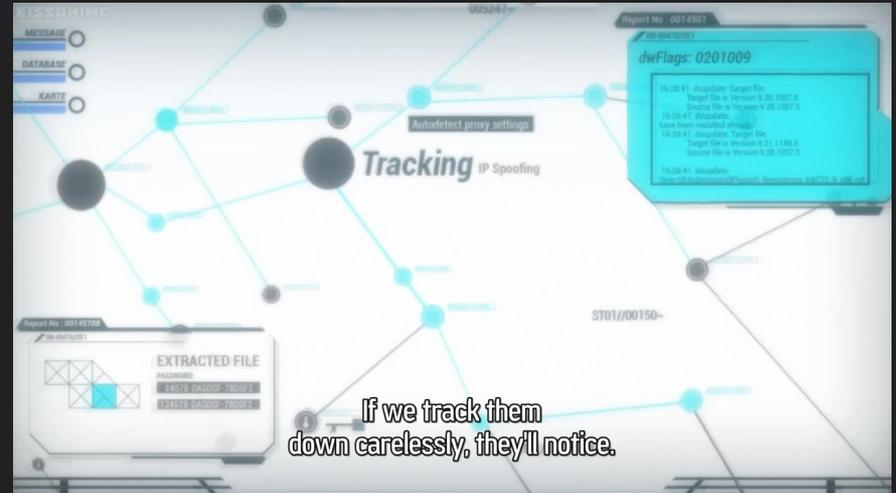
LEVEL 1: Cleaning up your messy room
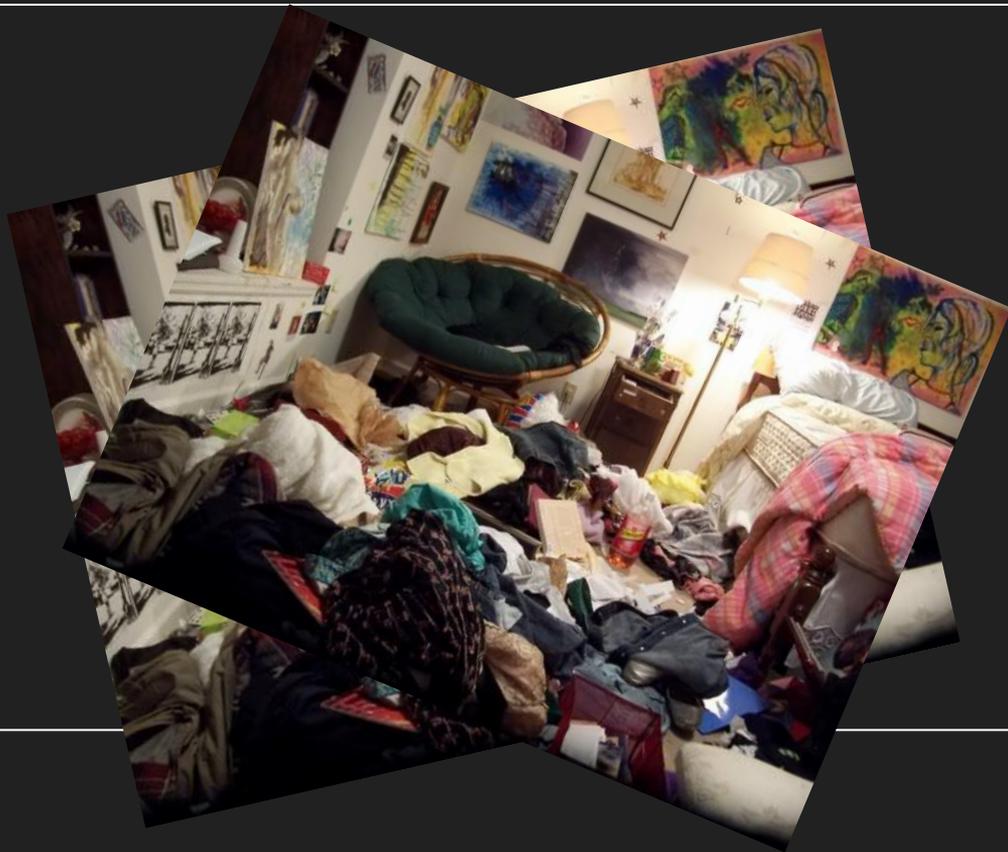
Everyone is FINGERPRINTABLE!

What is Incognito Mode?

Blocking cookies and deleting

 search histories,

does it even matter?

https://panopticlick.eff.org/

Search with Something Else

Google, Bing, Yahoo all make money by tracking your searches and feeding you ads. TRY USING SOMETHING ELSE!!!

- DuckDuckGo
    - https://duckduckgo.com
- Startpage
    - https://www.startpage.com/

Locking down your browser

WHO is tracking you?

- Corporations
- Government agencies
- Personal or political adversaries

Lets see those corporations at work! →

- Firefox w/ Lightbeam

Block those trackers!

- Block trackers:
  - Disconnect.me
    - https://disconnect.me/
  - Privacy badger
    - https://www.eff.org/privacybadger
  - Ghostery
    - https://www.ghostery.com/
- Https Everywhere
  - https://www.eff.org/Https-Everywhere
- Do not track
  - http://donottrack.us/
- AdBlockPlus
  - https://adblockplus.org/
- No Script JS - https://noscript.net/

Did that help?

Try panopticlick again!

Try lightbeam again!
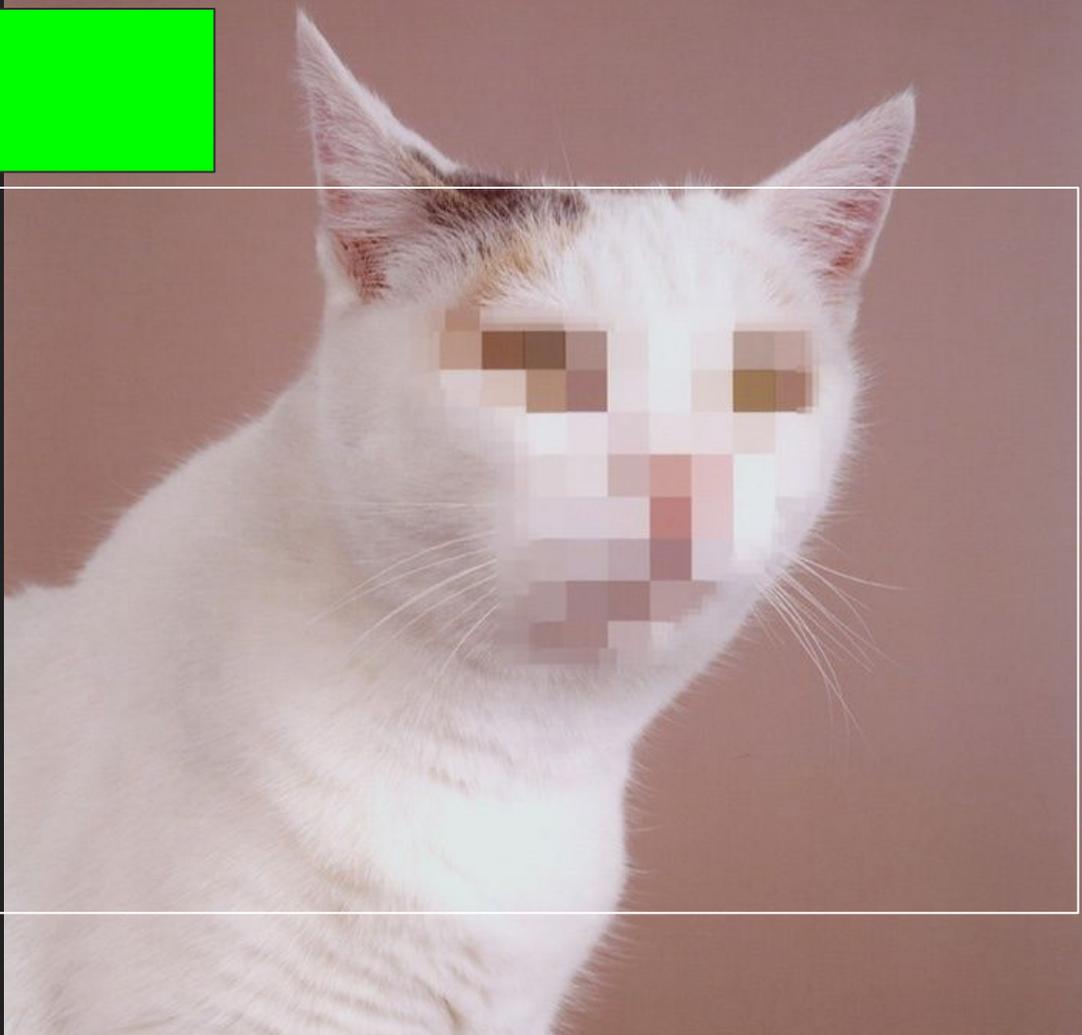
Locking down your Social

- Social settings, checking up on them
- Keep them in their own buckets, limit what facebook sees of you around the web

Physical Data

- Don't use a thumb print!
- Cover those cameras...
- Turn of location when you don't need it

Passwords!

- password managers
    - 1Password - https://1password.com/
    - LastPass   - https://lastpass.com/
    - KeyPassX - https://www.keepassx.org/
- Generating passwords
    - Dice ware - http://rumkin.com/tools/password/diceware.php
- Lock your phone with at least a 6 digit code

Encrypt your Hard Drive

It will take a few hours, so it is best to do it overnight!

FOR A MAC:

go to System Preferences> Security & Privacy icon > FileVault

Click on the lock icon and enter an admin name and password

Click on Turn On FileVault button

FOR A PC:

go to Control Panel and choose System and Security.

Click the BitLocker Drive Encryption.

Turn on BitLocker next to the drive you want to encrypt

LEVEL 2: Pulling up your hoody

Level 1 Vulnerabilities

- I.P. address still visible - physical location
- Still fingerprintable by specifics of your computer
- Reduces data, not anonymizing

Level 2: Anonymity Light

MESSAGING (sexting) 101

- All txt messages can be picked up at cellphone towers.
- Something as simple as apple's iMessage at least encrypts your messages so that they can't be heard over the network ***
- Skype / WhatsApp / iMessage are good, but the companies have the keys
- SIGNAL !
  - Open source
  - 3rd party verified
  - No 3rd key to unlock your messages
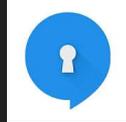
INSTALLL THAT JAM (download it from the app store)

Kill all location data from your phone

Faraday bags

Killyourphone.com

PGP email encryption

http://www.gpgtools.com

TOR

How it works! Why it exists!

https://www.torproject.org

Let's go visit the hidden wiki!
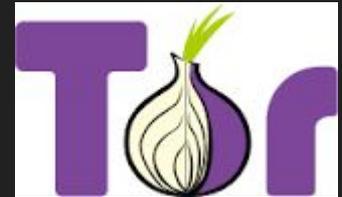
LEVEL 3: Becoming Anonymous

Level 2 Vulnerabilities

-Anonymizing but still anonymizing your own identity

E.g. PGP Email encrypts your email, but it's still your email address

Level 3 we begin to build new identities

Alternative computing devices

- Cash for computers on craigslist
- Public computers
- Burner phones

Finances: Buying Bitcoins Anonymously

-Moneygram at CVS using cash to a bit-wallet in anonymous email address

Crafting Alternative Identities

- Utilizing the postal service: ANONYMOUS LETTER BOXES
- http://status.irational.org/letter_box/
- Getting other email addresses
- Building social networks
- Getting identification

To judge him, we need to measure his Psycho-Pass as a collective entity.

TAILS

-The Amnesic Incognito Live System

-Boots onto windows computers

-Amnesiac so nothing you do in Tails will be saved to the computer (doesn't include web activity)

-High Level of Anonymity

Vulnerabilities

-committing a crime

-still vulnerable to high level surveillance e.g. cia, FBI,

- genetic material http://deweyhagborg.com/