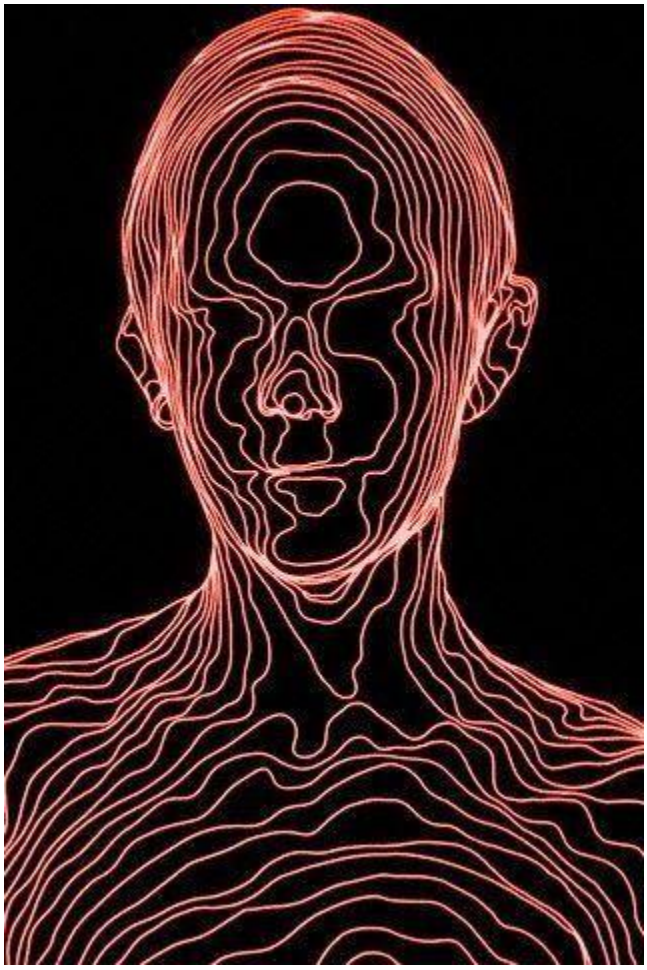
The Whistleblower's Guide



Ollie Hogue

Table of contents

What This Guide Will Be About (The Criteria)

Here is the pseudocode of the guide:

```
for i in [whistleblower tools]:

      Explain how they work

      Try to implement them myself
```

What are the `[whistleblower tools]`?

- Private operating system.
- Tools used to hide from surveillance
  - I cover private browsing (Tor) private messaging apps (Signal).
- Malware programs that download all the existing contents from a computer.
- Steganography encryption and decryption tools.
  - I make a case that the deep web is similar to Steganography in its security through obscurity, and explore deep web concepts instead.

Criteria Justification

For HD:

- Malware and steganography are explained in the final guide
- Final guide shows 3 or more uses of code to create models, modifications or proof of concepts.
  - *(see: python proxies, steganography website, python deep web brute force program)*
- Guide is clear, informative and interesting. Images included, jokes made, some diagrams where relevant:
  - *(see: this guide)*
- Writes all 6 blog posts. In the guide, writes about tails (private os), private browsing and private messaging in detail. Genuine attempts to implement tails, private browsing, and private messaging. Evident in blog posts.
  - *See the following blog posts:*
    - *Whistleblower platforms*
    - *Tails and Private Browsing*
    - *Private Messaging*
    - *Steganography with code pt. 1*
    - *Steganography with code pt. 2*
    - *Tor coding model*
      - *Related Articles and Films to watch*
      - *Reflection on whistleblowers and insiders, with further reading links*

Private Operating System (Tails)

What is Tails and how does it work?

- Tails is an operating system (like windows and linux) except it is secure and runs off your USB.
    - The USB doesn't use the Hard Drive, so any existing viruses there won't be enabled.
    - However, If you installed tails from a computer with a virus, the security of tails might be compromised.
- Tails lacks persistency (it is amnesic). It lives in RAM. This all means it does not write to the hard drive unless strictly specified.
    - With persistency (aka on an average OS), websites files and passwords and leave traces on your computer
    - Tails CAN use persistent storage and save files with Encrypted Persistent Storage.
        - The encrypted space is not hidden, but its data is not distinguishable from random data, providing plausible deniability.
- Secure software are already installed onto Tails, so internet browsing is safe:
    - Tor is installed (secure internet browsing, explained later)
    - OnionShare, to share files over Tor.
- During shutdown, Tails will overwrite most of the used RAM to avoid a cold boot attack
    - A cold boot attack is where an attacker performs a memory dump on the computer's RAM to retrieve encryption keys from an OS.

How I implemented it

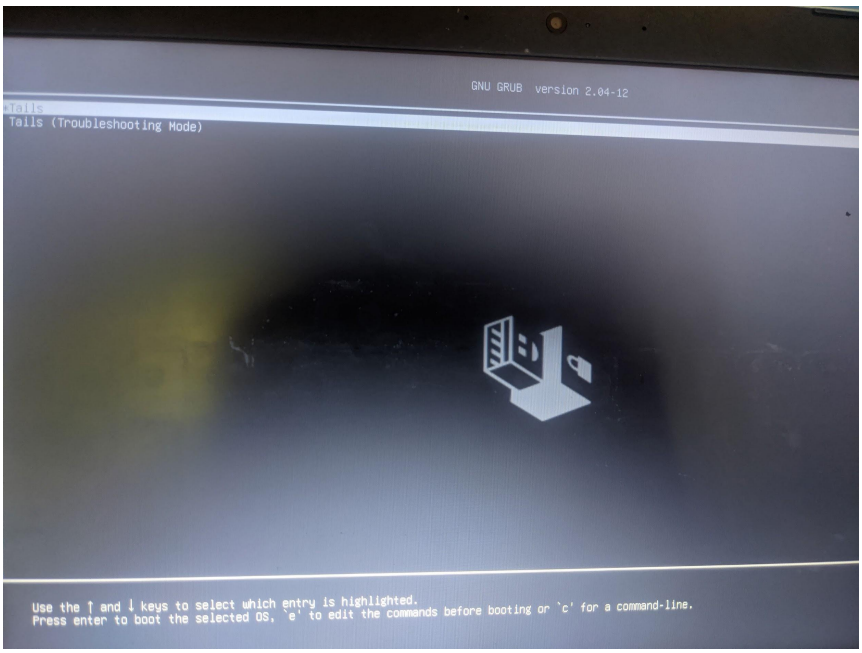
First I visited the tails website, downloaded the "image" of the operating system, and flashed it to a usb using the unix command:

```
sudo dd if=/file_directory/tails-amd64-4.16.img of=/dev/sdb bs=16M
oflag=direct status=progress
```

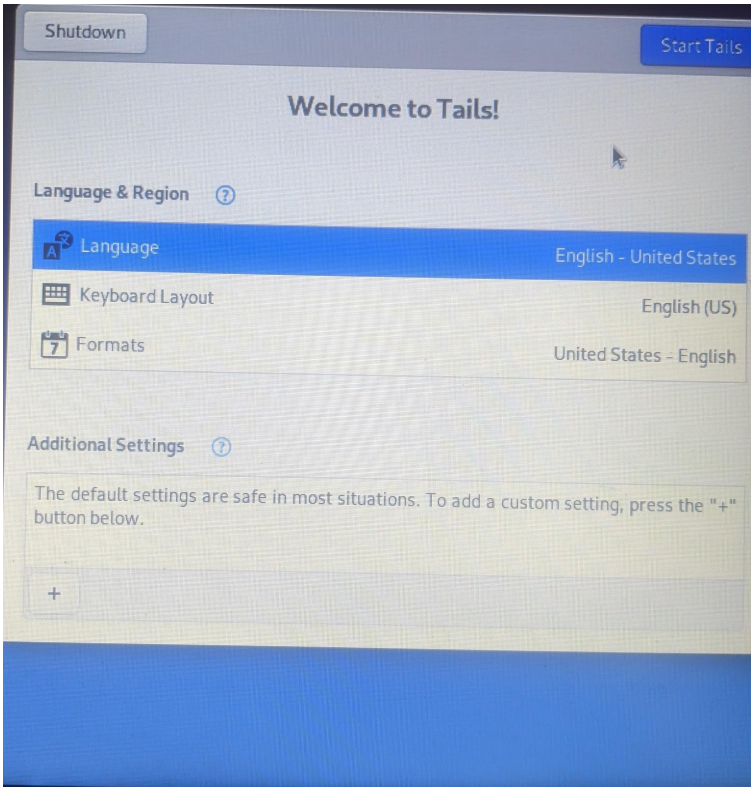
The tricky part for me was trying to boot my computer from USB. I was supposed to open up the boot menu (by pressing f10, f12, or esc, depending on my computer model. Then I needed to select "USB", and supposedly tails would run. I was able to open it by the boot menu, but everytime after making my selection, normal booting up would start.

I used the troubleshooting menu of the website which suggested reinstalling tails to the usb, or a new usb, or trying a new computer. I tried a nearby computer, but I was unsuccessful in opening the boot menu.

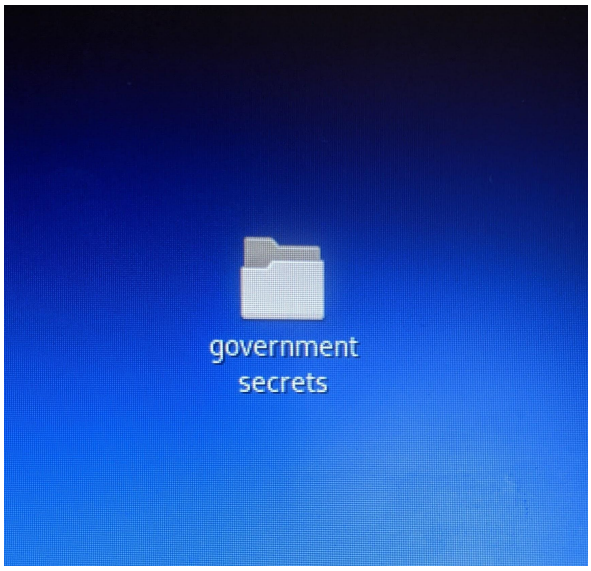
I flashed tails to a new USB. I eventually learned that I needed to be precise in pressing f10, f12, OR esc. Previous I have been barbarically bashing them all until I heard a loud beep. This time I only pressed the recommended one for my model, and it worked!! Tails was being booted!



Next I set up the language and wifi:



Then I set up permanent storage, meaning that some files and settings will stay with the USB each time it is booted (if they know my passphrase). There were a few security warnings with this setting, so I will carefully consider whether to actually use it.



Private Browsing (Tor)

How it works

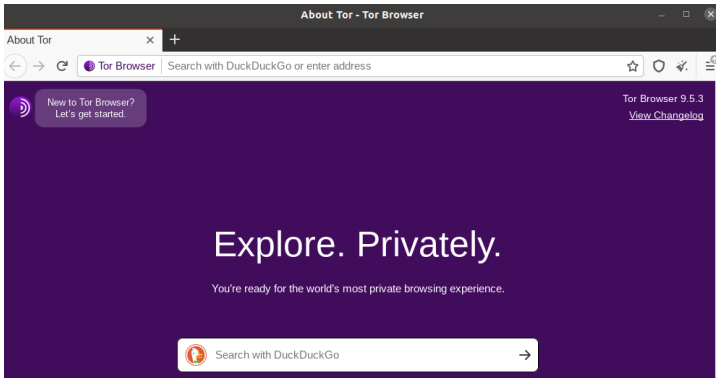
- Tor is a layering service. Tor encrypts the connection by passing it through 3 different servers hosted by different people and organizations around the world. Each server (called a relay) doesn't know where the connection is coming from and where its going
- This way the system is secure even if a single relay is malicious.

A Harry Potter (fanfic) analogy:

That had been a Slytherin System delivery, what you used if you wanted to communicate with someone without anyone else knowing that the two of you had talked. The sender gave an envelope to someone who had a reputation for being a reliable messenger, along with ten Knuts; that first person would take five Knuts and pass the envelope to another messenger along with the other five Knuts, and the second messenger would open up that envelope and find another envelope with a name written on it and deliver that envelope to that person. That way neither of the two people passing the message knew both the sender and the recipient, so no one else knew that those two parties had been in contact...

How I implemented it

Tor is a free private browsing service. It is automatically installed on tails, but I also installed it on my normal operating system so I can experiment..



Coding Example #1 - Mimicking aspects of Tor using proxies

A proxy allows a user to contact a website indirectly, by going through a middle man (proxy server). Your original IP address is then hidden, and the proxy's IP address is used.

Here I will code a proxy so we can start understanding what that means. My code sends traffic through two proxies, and then tries to access my website.

The key differences between my program and Tor are that

- My program checks if a website exists, it doesn't show it to the user like a browser.
- Tor uses encryption and creates secure tunnels between a user and its proxy. NO extra encryption is added in my program.
- Tor passes traffic through at least 3 different servers, like three different proxies, with a separate layer of encryption for each of the relays. My program passes through 2.

```
My real IP is...
{'origin': '203.40.187.30'}
website at https://httpbin.org/ip recognises my IP as:
{'origin': '15.185.193.6'}
Web site https://ollieiswoke.github.io/favourite-things/ exists, checked through proxy
```

```python
import requests

url = 'https://httpbin.org/ip'
proxies = {
    "http": 'http://5.252.161.48:8080',
    "https": 'http://15.185.193.6:3128'
}
real_response = requests.get(url)
print("My real IP is... ")
print(real_response.json())
print("Now activating proxies...")

response = requests.get(url,proxies=proxies)
print("website at https://httpbin.org/ip recognises my IP as: ")
print(response.json())

url = 'https://ollieiswoke.github.io/favourite-things/'
request = requests.get(url, proxies=proxies)
if request.status_code == 200:
    print('Web site {} exists, checked through proxy'.format(url))
else:
    print('Web site does not exist')
```

What can we learn from this model?

- Running this code took about 10 seconds when I added the proxy servers. This helps contextualise why Tor is known for its slow browsing experience: using multiple proxies slows down loading time.

Sources:

- https://whatismyipaddress.com/tor
- https://support.torproject.org/about/how-is-tor-different-from-other-proxies/
- https://www.expressvpn.com/what-is-vpn
- https://www.scrapehero.com/how-to-rotate-proxies-and-ip-addresses-using-python-3/
- https://stackoverflow.com/questions/16778435/python-check-if-website-exists

Private Messaging (Signal)

Okay, let's pretend I work at a company, and have successfully extracted Secrets™. How do I tell people? Share the files? aka how does private messaging work?

What is Signal?

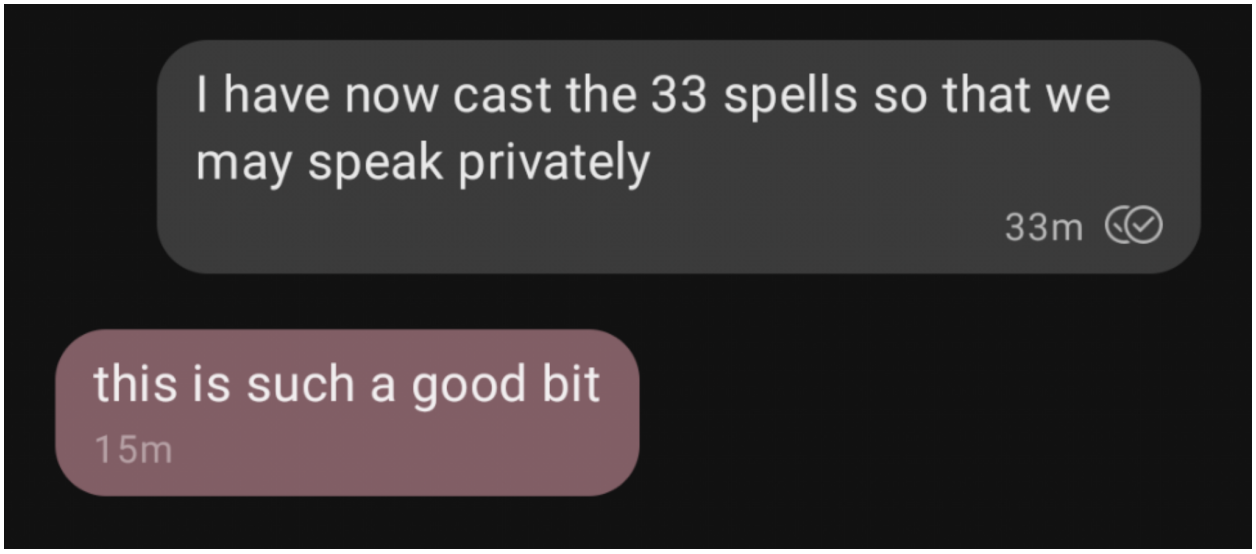
Signal is a private messenger app. It was the most downloaded app in the US after the riots. It is one of the few apps that has been endorsed by Edward Snowdin.

How does Signal work?

- Signal uses **end to end encryption**, which means the data is encrypted on its entire journey, and the cryptographic keys are stored exclusively at the endpoints. This means the third parties in between (eg internet service provide, application service provider) are not able to read the data
    - The implication of this is that if police asked the Signal company for your message history, they wouldn't be able to see the actual messages. For example in 2016, a grand jury issued a subpoena for signal Signal data, but only could get the user's register and the last time they used it.

How to use Signal? a demonstration

- I installed Signal from the app store, super easily.
- Keep in mind, your friends can see you have a signal account.
- Anyone who has your phone number can tell whether you use Signal. If you were to do REAL cyber crimes, you would have to take extra precautions, such as using a burner phone.
    - These details are discussed here.
- So once I downloaded Signal, I chose a username, and found contacts through my contacts



Malware (Via USB)

How would a whistleblower use malware? In many cases, the whistleblower is an insider who has unique access. Others around you think you are on their team, and thus show may already have given you access to valuable systems.
What if you are in a company, but not well respected? What if you are a spy-janitor at NASA? There are situations where one might have physical access, but not passwords. This is where USB malware comes into play.

How it works

USB's can 'auto-run' programs when they are plugged in, without admin permission etc.

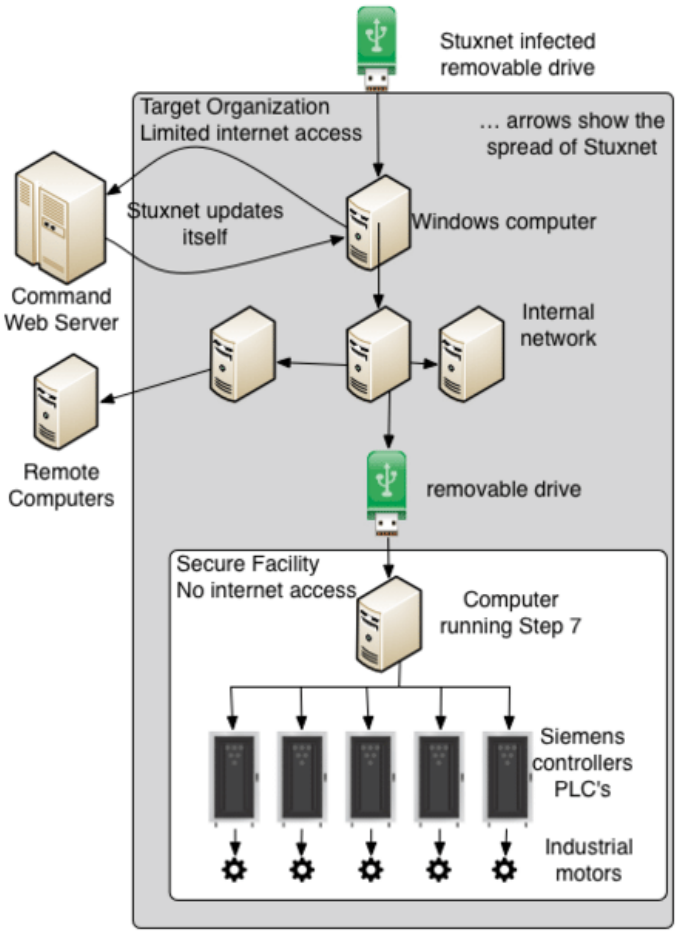
- Therefore, a malicious USB stick could install all sorts of malware, such as backdoors, trojans and information stealers.
- Auto-run is restricted on Windows 7 and higher, but there are other devices that may not have this setting.
- One weakness that USB attacks can exploit - curiosity. In 2016, researchers from University of Illinois left 300 unmarked USB flash drives around campus, and half of them were plugged into a host's device to try and access the content.

A small case study, the stuxnet worm:

The Stuxnet worm was a malware program that used to cause damage to Iran's nuclear program. It exploited programmable logic controllers (industrial computers used to control robotics) causing the fast-spinning centrifuges to tear themselves apart.

The PLC computer model that was corrupted

The virus was introduced to the environment via USB, which contained Windows shortcut files to initiate compromising code, The worm that used other exploits to infect and update other computers inside the network with the virus. Note that 4 different zero days were exploited in this virus, assisting greatly in the process. A zero day is a software vulnerability that the defender doesn't know about and hasn't accounted for.



~~Steganography~~ The Deep Web

What Steganography and how does it work?

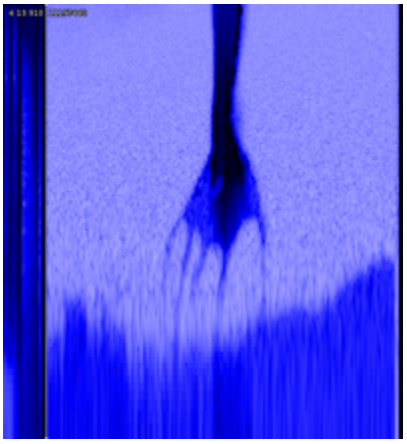
Steganography is the technique of hiding a message within a message, or more accurately, hiding that there *is* a secret message. Physical examples include:

- Secret messages in invisible ink
- Hidden messages amond words of a less suspicious cover text (called a null cipher). Eg the first letter of each of these kirby worlds spelling out C-R-O-W-N-E-D

- Messages written on envelopes in the area covered by postage stamps.

Often this is seen as in computer files, messages, images, or videos.

- Hiding data in the lowest bits of noisy images or sound files (that usually aren't detected).
- An image or a text can be converted into a sound file, which is then analysed with a spectrogram to reveal the image. Eg. the Nine Inch Nails Album cover if decoded through their song "My Violent Heart"



Is the Deep Web similar to Steganography?

I would argue yes:

- Instead of hiding valuable information within computer files, messages, images, or videos, it is hidden in a website domain.
- To a whistleblower, they would use it for similar reasons - to hide information.
- Only people who know the secret can get the information
- Both are a form of security through obscurity, where its power comes from everyone keeping secrets.

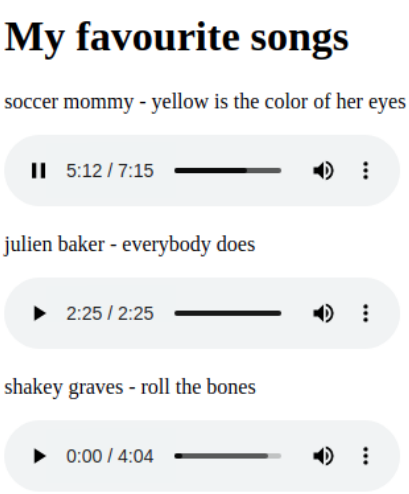
Using the deep web to hide information:

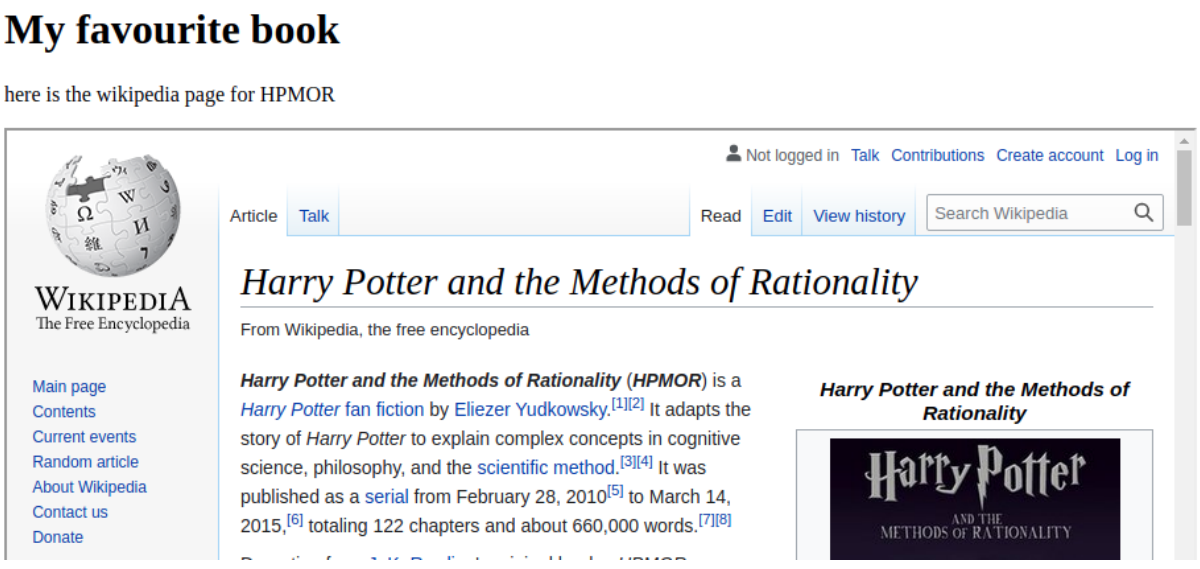
Coding Example #2, making a steganographic website

For the technical aspect of my project, I started coding a website that uses Steganography to hide valuable information.

The concept is simple: I am a whistleblower and I send you a seemingly innocent website. BUT if you and me both know that there is a secret (and what it is), we can find secret information.

The website I made is here: https://ollieiswoke.github.io/favourite-things/





Looks normal, right?

BUT if you know that there is a secret subdomain to the website, you might find this:

you have found the secret!

this is an analogy for the dark web

How would you figure out the secret web domain, without any additional information? Find out below **eyes emoji**.

Coding Example #3, making code to unlock a hidden part of a website

If you *know* there's a secret domain on a website, how would you find it?

Here is a tool I coded that brute forces subdomains to detect any secret ones.

```
import requests
import sys
import itertools
domain = sys.argv[1]

#for the first 20 characters
char_set = ''
for i in range(33,127):
    char_set += chr(i)

print(char_set)
for i in range(12):
    for subdomain in map(''.join, itertools.product(char_set, repeat=i)):
        #ignore domains like instagram.com/#asdsadsa
        if subdomain[0] != '#':
            website = domain+'/'+subdomain
            request = requests.get(website)
            if request.status_code == 200:
                print('website found at:', website)
```

Using it on my website, I haven't gotten any useful information for the first ten minutes, the program is still cycling through the first 4 character combinations. I am expecting this to take all night, or possibly longer.

How is this like the dark web?

- Websites on the Dark web are also part of the deep web: the part of the Web not indexed by web search engines
- Content of the deep web may be accessed by an IP address or URL, but may also require a password to bypass a HTTP form.
    - Eg Netflix, and your banking details are part of the deep web, can't be accessed just with the URL, also need to fill out a form with a password.

        - For the sake of simplicity, my Deep Web proof of concept didn't have a password.
    - An important distinction - my proof of concept is of the deep web, if it was of the dark web, it would have to be accessed via Tor (source).

How *secure* is the dark web?

- This brute forcing technique works, but it takes *ages,* that's why this technique can't normally be used to identify all dark websites.

The dark web is inefficient to brute forcing entry, but the question is, is *that* its weakest link? I have a strong inkling convincing a criminal to show you the dark websites they know will be quicker than brute forcing it. If you appear to them as a completely normal criminal, they will not be able to stop you. This reinforces the power of insiders.

Evidence for this claim: looking up the dark web, I found this website that had dark web listings.

Bonus - Extra reading

Legal Advice

Australians has whistleblower legislation that should protect them, see here.

General:

The whistleblowers handbook - much more in depth, covers most common pitfalls.
An article on another whistleblower book - Axis of deceit

Platforms to Reveal information

See this blog post.
Too platforms to consider and GlobalLeaks and SecureDrop

- Claims the two standard platforms for whistleblowers are GlobalLeaks and SecureDrop
    - SecureDrop is a two way system where media companies and NGos can install it, and anonymous people can upload leaks to the browser. This is something I can experiment with later.
        - Importantly, they recommend using TOR when uploading (though I think VPNs would work too)
    - Global Leaks
        - Has a chat system with whistleblower
        - Has a nice section explaining different use cases for whistleblowing.
        - Also used from the web browser
        - Has a Demo to use with Tor