Ethical Student Hackers

Anonymisation + TOR



EGM



The Legal Bit

- The skills taught in these sessions allow identification and exploitation of security vulnerabilities in systems. We strive to give you a place to practice legally, and can point you to other places to practice. These skills should not be used on systems where you do not have explicit permission from the owner of the system. It is VERY easy to end up in breach of relevant laws, and we can accept no responsibility for anything you do with the skills learnt here.

- If we have reason to believe that you are utilising these skills against systems where you are not authorised you will be banned from our events, and if necessary the relevant authorities will be alerted.

- Remember, if you have any doubts as to if something is legal or authorised, just don't do it until you are able to confirm you are allowed to.

- Relevant UK Law: https://www.legislation.gov.uk/ukpga/1990/18/contents



Code of Conduct

- Before proceeding past this point you must read and agree to our Code of Conduct - this is a requirement from the University for us to operate as a society.
- If you have any doubts or need anything clarified, please ask a member of the committee.
- Breaching the Code of Conduct = immediate ejection and further consequences.
- Code of Conduct can be found at **shefesh.com/conduct**



Anonymity

Anonymity - remaining unknown

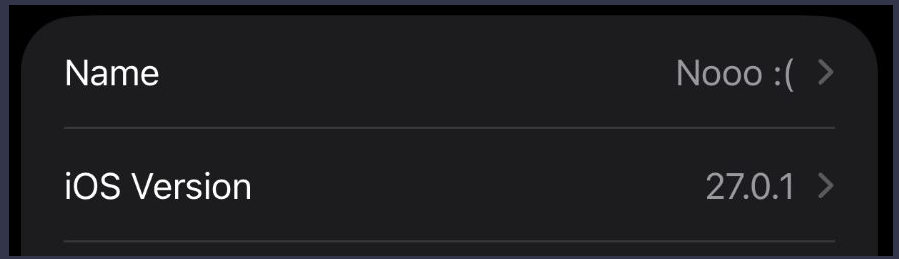
On the internet

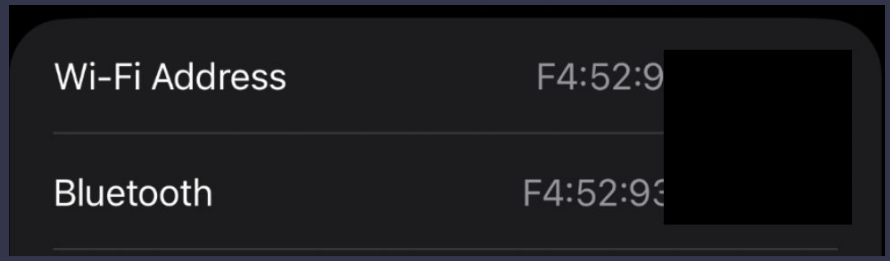
- Usernames
- Fake information in forms
- Throwaway emails
- VPNs
- Public wifi
- Privacy OS
- Rotating MAC Addresses
- Browsers
- etc

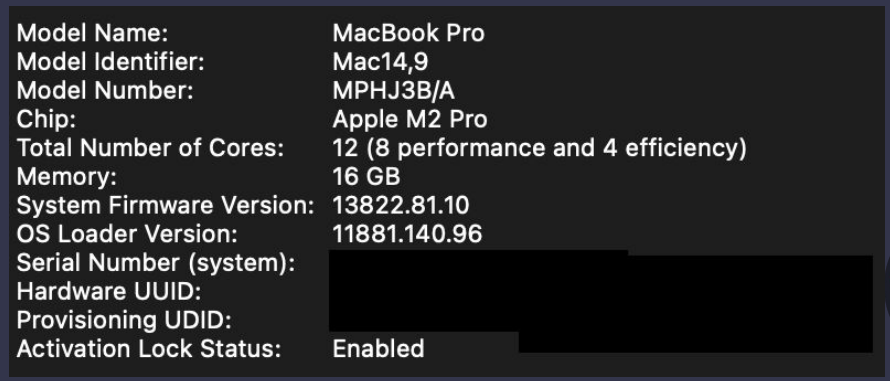
Benefits	Drawbacks
Freedom of expression	Can facilitate threats and abusive speech
Protection of identity	Can create a false sense of security
Reduced social pressure	Can reduce accountability
Freedom to experiment	Can enable impersonation and deception
Protection from surveillance	Can make it harder to investigate harmful behaviour

Device Anonymity

- Device Name (hostname)
- MAC Address
- Bluetooth Name + MAC
- OS Version
- Services running
- IMEI
- Network Provider
- Telemetry
- Etc





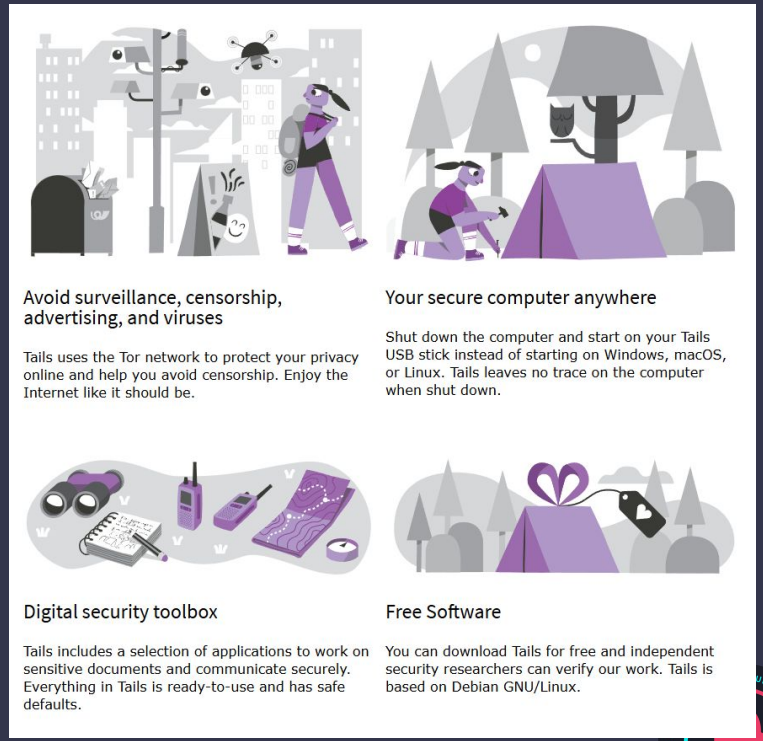


TAILS OS

The Amnesiac Incognito Live System (TAILS)

- Security focused Linux Distro

- **Amnesiac** - OS fits into system RAM meaning it never touches any persistent storage
- **Incognito** - TOR as standard, encrypted emails, encrypted storage
- **Live system** - designed to be booted off a USB stick

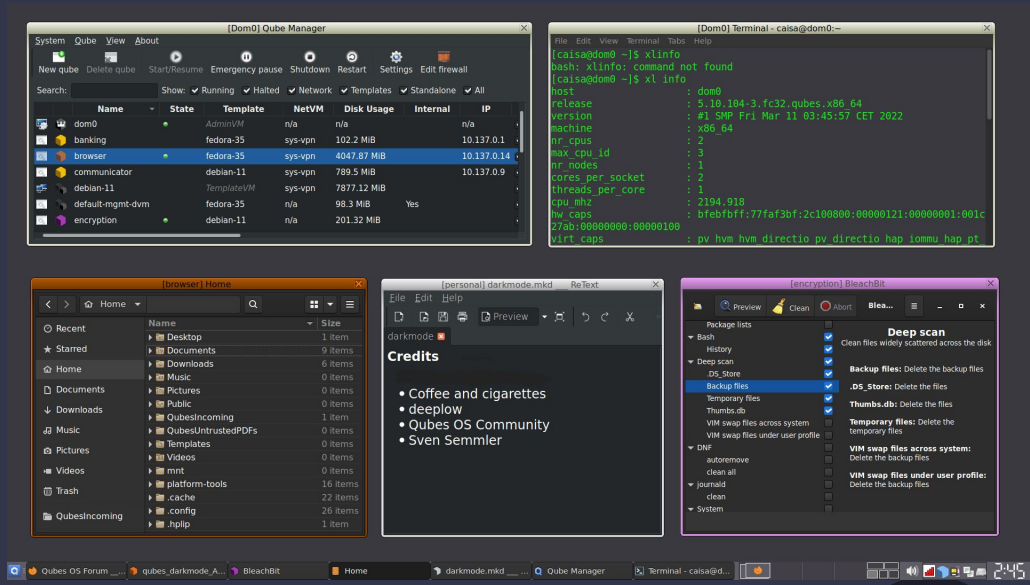


QUBES

More Security than Anonymity focused
- Another Linux Distro

‘Qubes’
- Isolated environments
- Separate apps / network connections / data
- No access between environments

Zero-Trust Architecture



GrapheneOS

Modified Android OS

- Hardened Android Kernel
- MAC randomisation
- Identifier protection
    - Reduces leaks of device identifiers
- Greater privacy controls
    - Restricts access to the network, files, contacts, clipboard, etc
- Strips out reliance on Google
    - Optional + Sandboxes



SHEFFIELD ETHICAL STUDENT HACKERS

Network Anonymity

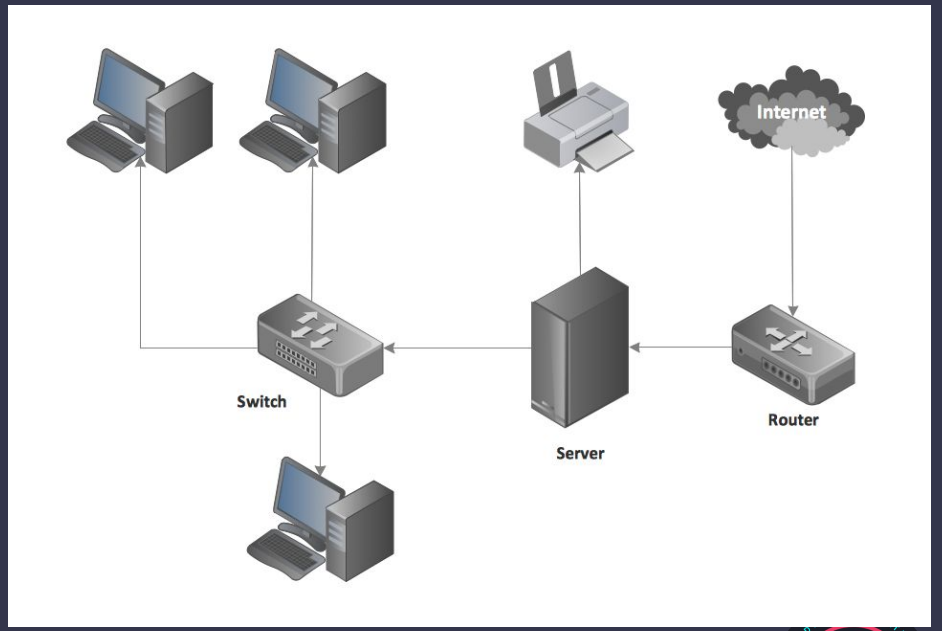
Sending data over the network comes with identifiers

Local Network:

- MAC Address (63:31:B0:D4:D6:98)
- Private IP Address (192.168.3.112)

Internet

- Public IP Address (143.167.2.123)
- Destination IP (142.250.151.113)
    - This is the site you're visiting



What you're sending is protected by HTTPS

ISP

Internet Service Provider

- BT, Virgin, EduRoam, ASK4
- Provide the connection between your local network + wider internet

Required by UK law to store data about you

- Customer account identifiers
- Source IP + Destination IP address
- Connection timestamps
- Website domain names
- Data transfer volumes

Can be looked at by government organisations



TOR

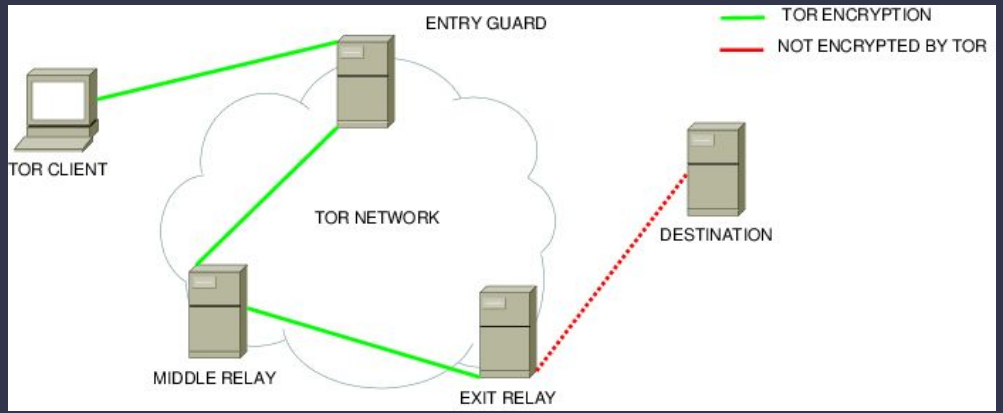


What is TOR?

TOR stands for **T**he **O**nion **R**outer

Onion Routing

- Different ‘layers’
- Routes traffic between 3 servers
- Each server only has knowledge of previous server + next destination



Dark Web vs Deep Web

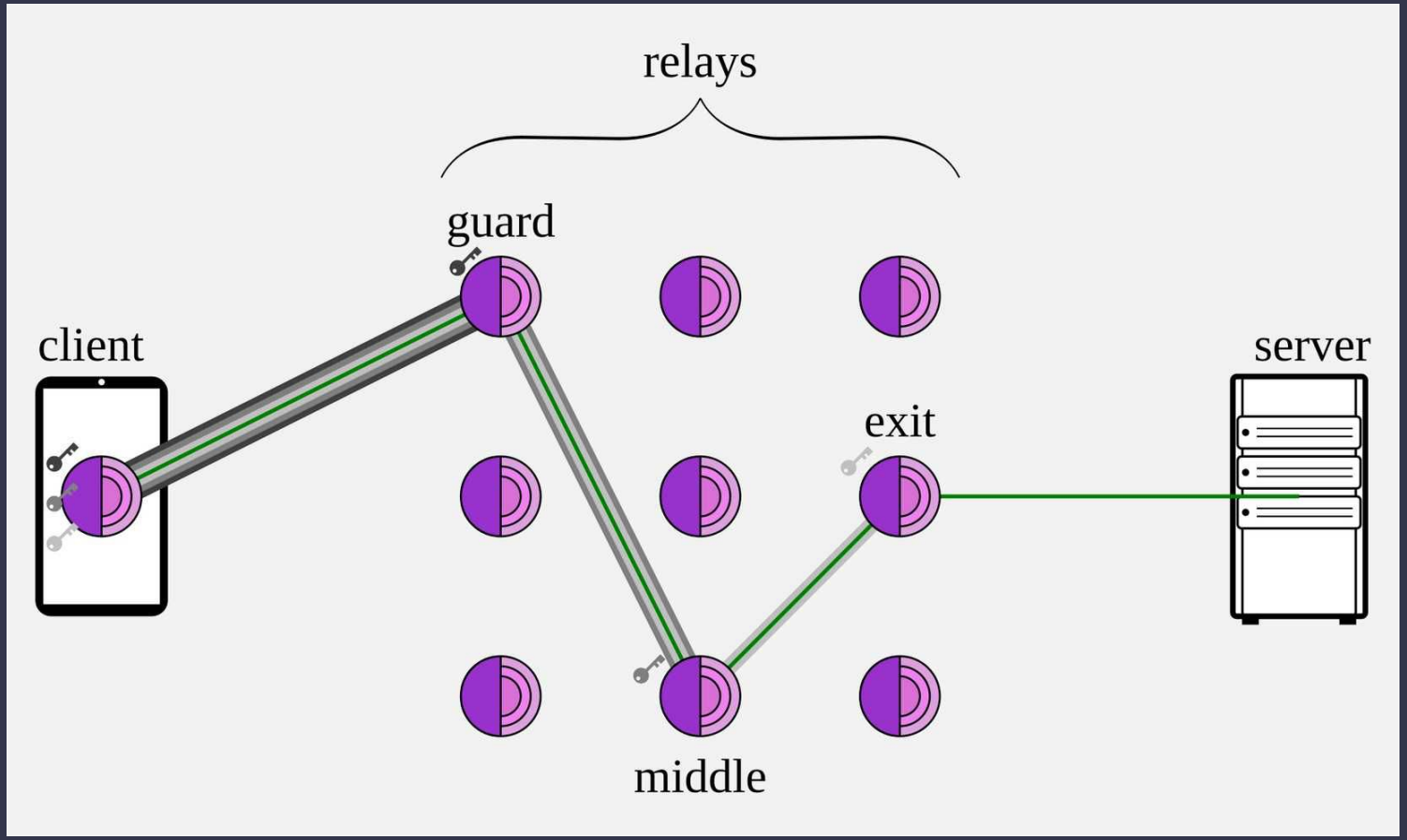
Deep Web
- Sites that cannot be indexed by web crawlers
  - Internet Banking
  - Email inbox
  - Medical documents

Dark Web
- Subsection of the Deep Web
- Websites that can only be accessed through purpose-built web browsers
- Main application is to provide anonymity to website owners and visitors

Accessing the ‘Dark web’ is NOT illegal in the UK
- What you access on it could be

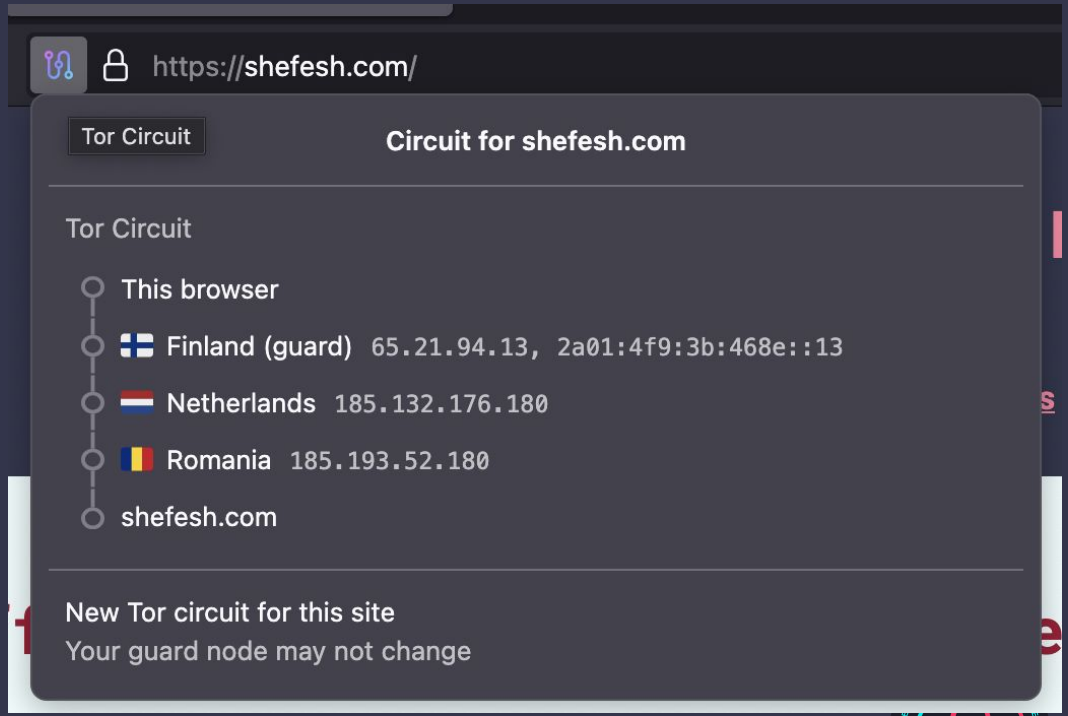


3-Node System



Why does it work?

- Layered encryption
- Distributed relay network
  - Relays (Nodes) operated by different parties
- Circuit (Path) changes constantly
  - Can also manually shift it too
- Distributed trust
  - No single relay knows both the receiver IP and server IP
- Resistant to traffic analysis



Possible Risks

Exit node cannot protect unencrypted traffic

- If the end server is not configured / not configured properly to use HTTPS

Relays are not necessarily dependent

- Law enforcement / Security services known to run entry + exit nodes

Guard reuse

- Guard tends to stay stable - allows for traffic correlation

E2E Traffic Correlation

- Possible to correlate timing + volume to associate services with users

Anonymity can fail regardless

- Identifying in messages, malicious downloads, etc
- TOR hides the search but can't protect from human stupidity!



TOR Uses

There are many reasons why you'd want to remain anonymous whilst accessing certain parts of the web

- Conducting OSINT
- Federal Investigations
- Preventing tracking
- Cryptocurrency transactions
- Whistleblowing
- Criminal Uses (BAD)

TOR Practical

Download the TOR Browser https://www.torproject.org/download/

1. Use to connect to a surface website (like sheffield.ac.uk / shefesh.com)
2. Connect to a Tor hidden services website and see what is different
   a. bbcnewsd73hkzno2ini43t4gblxvycyac5aw4gnv7t2rccijh7745uqd.onion
   b. duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswzczad.onion
   c. reddittorjg6rue252oqsxryoxengawnmo46qy4kyii5wtqnwfj4ooad.onion
   d. g7ejphhubv5idbbu3hb3wawrs5adw7tkx7yjabnf65xtzztgg4hcsqqd.onion



Browser Anonymity

Every Browser has a **‘fingerprint’**

- List of characteristics unique to a user, their browser, and their hardware setup

This fingerprint consists of:

- Installed fonts
- Screen resolution
- Time Zone
- Device platform
- And loads more

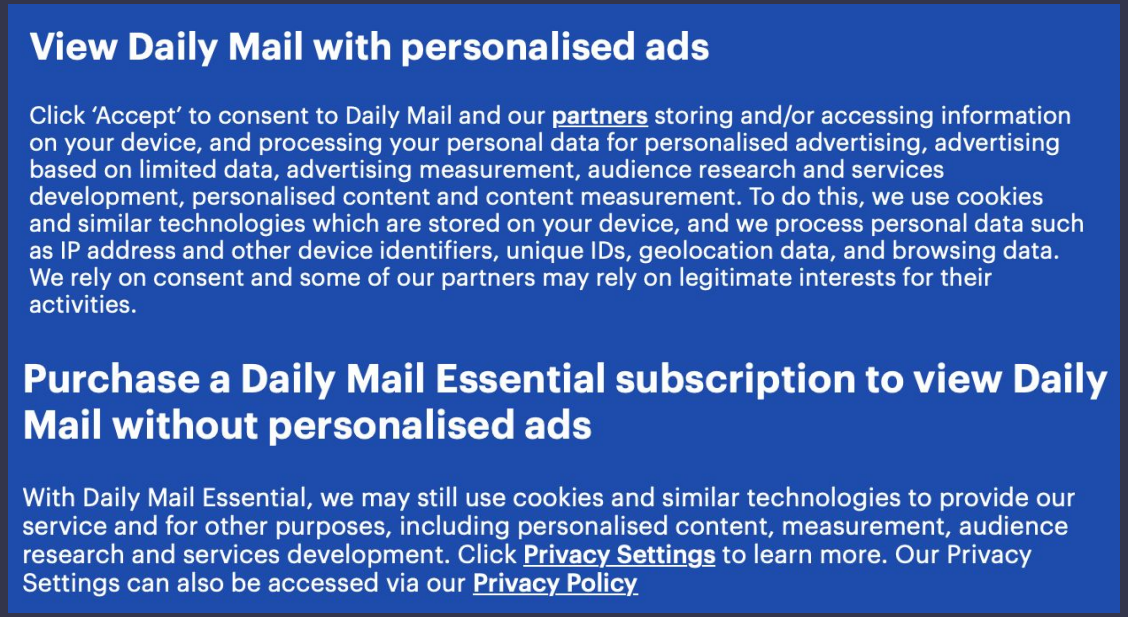
Uses JavaScript canvas - data about GPU, Browser, JS engine, etc



Why?

Companies want to track you!

- Advertising
- Anti-spam
- Account protection
- Analytics



View Daily Mail with personalised ads

Click 'Accept' to consent to Daily Mail and our **partners** storing and/or accessing information on your device, and processing your personal data for personalised advertising, advertising based on limited data, advertising measurement, audience research and services development, personalised content and content measurement. To do this, we use cookies and similar technologies which are stored on your device, and we process personal data such as IP address and other device identifiers, unique IDs, geolocation data, and browsing data. We rely on consent and some of our partners may rely on legitimate interests for their activities.

Purchase a Daily Mail Essential subscription to view Daily Mail without personalised ads

With Daily Mail Essential, we may still use cookies and similar technologies to provide our service and for other purposes, including personalised content, measurement, audience research and services development. Click **Privacy Settings** to learn more. Our Privacy Settings can also be accessed via our **Privacy Policy**

You agree to this in the terms + conditions (cookie popups)

- Might not even need to agree under some circumstances!!!

How to avoid fingerprint

Fingerprint resistant browsers (Brave, Librewolf)
- Can make you more obvious!

Standardised values
- TOR Browser does this

Tracker blocking (Ublock)

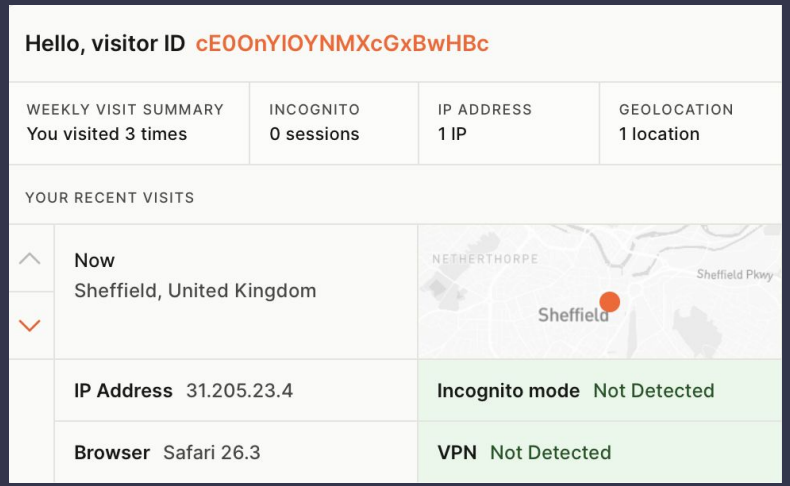
Avoid uncommon browser extensions
- These will change your fingerprint!



Browser Anonymity

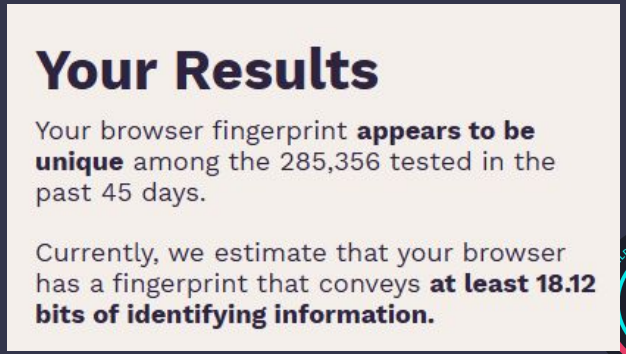
coveryourtracks.eff.org

fingerprint.com









Any Questions?



www.shefesh.com

Thanks for coming!



TOR TRYHACKME

https://tryhackme.com/room/torforbeginners

