Cryptography & Darknet

Workshop 9 – 26.9.2025

Senate Select Committee on Intelligence

March 12

- “those who would want to weave the story that we have millions or hundreds of millions of dossiers on people, is absolutely false.... From my perspective, this is absolute nonsense”

Ron_Wyden_and_James_Clapper_-_12_March_2013.webm

The director of national intelligence, James Clapper directly lying under oath to Congress was Edward Snowden's breaking point that caused him to whistle-blow.

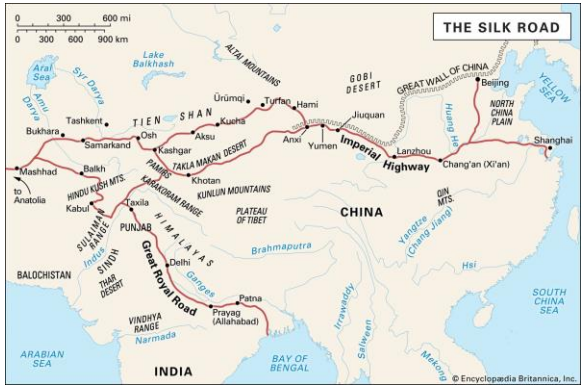
Snowden then quit his NSA/CIA contractor job at Dell to work at consulting firm Booz Allen Hamilton, where he sought employment solely to gather data and release details of the NSA's worldwide surveillance activity.

Snowden used Tails OS, running Tor browser where each of his messages were encrypted with PGP for additional security, to contact the press and send them documents revealing the spying the NSA has been doing all along.

Dread Pirate Roberts and Silk Road

The Dread Pirate Roberts was the alias used by Ross Ulbricht, the founder and operator of Silk Road, an online marketplace that allowed users to buy and sell illegal goods anonymously using Bitcoin

Silk Road operated much like any other e-commerce platform, with vendors listing their goods and buyers placing orders. However, Silk Road's primary focus was on illegal drugs, although other illegal products were also available.



Silk Road was a dark web marketplace that operated from 2011 to 2013, primarily used for the buying and selling of illegal drugs, fake IDs, counterfeit currency, hacking tools, and other illicit items.

Sending an unencrypted email through Google Chrome and Gmail

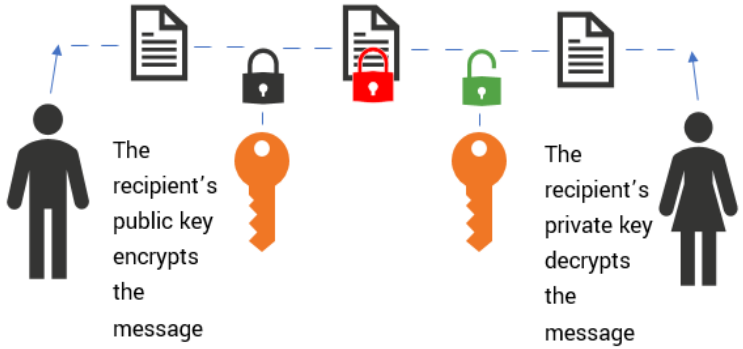
Chrome Browser	Gmail	ISP
Can see you've visited Gmail	Can see the content	The website, the sender, recipient, subject line, and timestamps,

With contents (PGP) encryption

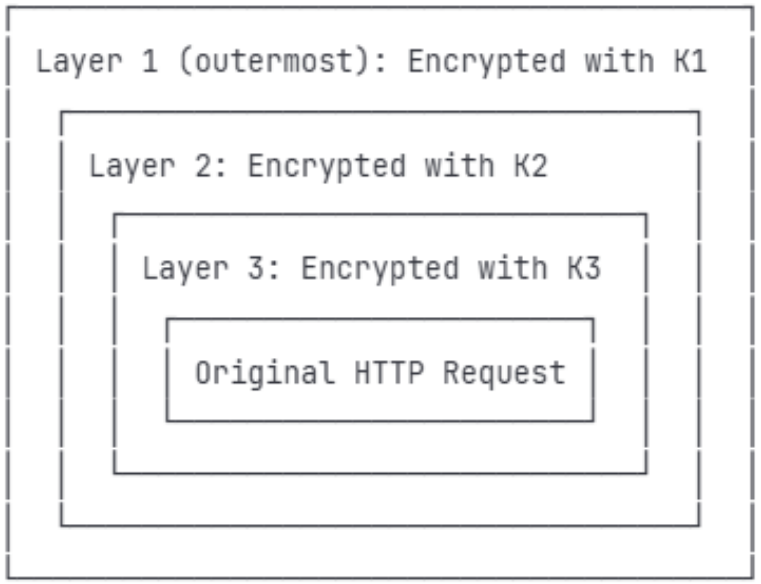
Chrome Browser	Gmail	ISP
Can see you've visited Gmail	Can see you sent a message but not content	The website, the sender, recipient, subject line, and timestamps,

With PGP encryption and a VPN

Chrome Browser	Gmail	ISP	VPN company
Can see you've visited Gmail (but not from which location)	Can see you sent a message but not content	Can't see anything exc ept your VPN IP	The website, the sender, recipient, subject line, and timestamps,



Your Computer	Internet Service Provider	Entrance Node	Relay Node	Exit Node	TOR Web server (the website)
Encrypts your packet with first the Exit node's public key, then the relay node's, then the entry node's key.	Knows you're connecting to Tor (sees Entry node)	Knows your IP but not your destination. Passes your packet to the Relay Node .	Knows the entrance and exit node but nothing else	Knows the destination but not who you are Sends fully decrypted data to the destination	Knows content of your request and sees exit node's IP, but, thinking it's the visitor.



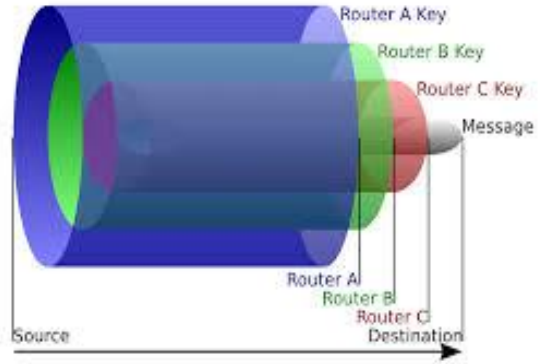
K1 = Entry Node
K2 = Relay Node
K3 = Exit node

Traffic going back to your computer is also encrypted, the same way but reversed.

The onion protocol

In short, the Onion Protocol used by Tor uses multiple layers and routing it through several relays (servers).

You want to send a message to Texas the location Ip is wrapped in serval layers



Packet will go to Paris
It then peels a layer of encryption sending It to Africa

Packet will go to Africa
Then peels off another layer sending it to
Going to Asia

Packet will go to Asia
It then peels of the final layer to the destination ip

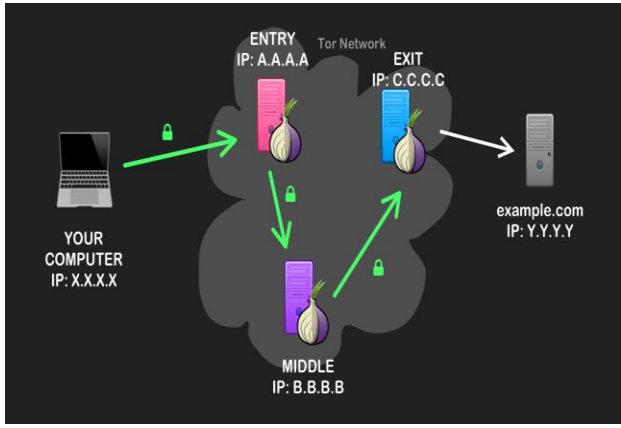
Packet then it will go to Texas
When it reaches Texas where it only knows it came from Asia but not the origin

Each relay only knows the previous and next relay, so no single relay can trace your origin or destination.

Why Onion?

Layered Encryption: When you send data through the Tor network, it is wrapped in several layers of encryption, one for each relay (node) in the circuit. Each relay can only "peel" off one layer of encryption at a time

- **Peeling Layers**: Just like peeling an onion, as the data passes through each relay, one layer of encryption is removed, until the final relay
- **Privacy**: Each relay only knows about the previous and next relay in the chain, so no single relay knows both where the data came from and where it's going.



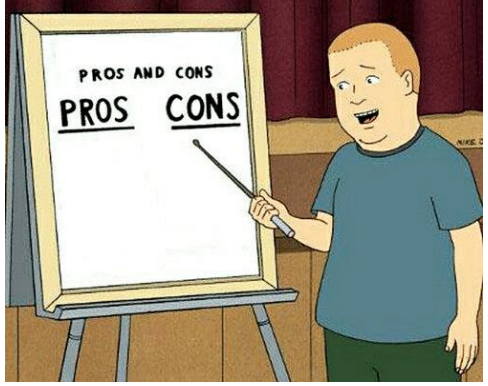
Mythbusters

- “Tor is illegal”
  - Tor is partly funded by the US State Dept, and the protocol was develoepd by the US Navy
- "Tor is only used for illegal things"
  - Most Tor traffic is used on clearnet sites
  - A major use-case of Tor is bypassing country-wide restrictions like in China and Russia.
- “Tor makes you 100% invisible”
  - Logging in (associating yourself with an account) and operational mistakes can still identify you

Statistics

- 2 million people use Tor daily
- 100k downloads every day
- Tor is becoming more and more mainstream – it is integrated into the Brave Browser
- 40%+ of traffic on Tor comes from BitTorrent

Pros and Weaknesses



- If not visiting HTTPS sites, the Exit Node operator can see your traffic
- This means they can steal passwords or inject malware

- If an adversary like the NSA controls both the entry and exit notes they can correlate packet timing to de-anonymise a user

- Zero-day exploits in Firefox can be found then used to reveal the user’s IP

Related

Browsers / Networks:

- **Arti**
  - Next-generation implementation of Tor written in Rust (instead of C)
- **Invisible Internet Project** *(I2P)*
  - *Internal network for hidden services. Can't access the 'Clearnet'.*
- **Hyphanet** *(formerly Freenet)*
  - *Distributed storage. Uploaded content is encrypted, split into chunks and spread across many user computers. Nobody knows what they're storing, and content persists after uploader goes offline. Designed for censorship-resistant publishing.*
- **ZeroNet** *(mostly abandoned)*
  - *Uses Bitcoin crypto and the BitTorrent network to host censorship-resistant websites.*
  - *Instead of an IP, websites are identified by public key (bitcoin address) and a private key allows the owner of the site to publish changes.*

Operating Systems

- **Tails OS**
  - Meant for use on a flash drive
  - Amnesic - resets back to a clean state any time you restart or unplug the USB.
  - Connects to the Tor network as a VPN by default for every application
- **Whonix**
  - Meant for use inside a virtual machine
  - Not amnesic
- **Kodachi**
  - Not much different
- **Qubes OS**
  - Designed for security rather than privacy.
  - Every application runs in its own virtual machine.
  - If one 'qube' is compromised, others remain safe.

Red Rooms

Live torture

People pay for the torturer to do things

can pay to watch—or even vote on—acts of torture or murder. They're often described as:

- Live video streams
- Controlled by criminals
- Viewers paying with cryptocurrency
- Audience deciding what happens

Not real maybe or are they hiding

There is no verified evidence that these livestreams exist. Cybersecurity experts, law enforcement agencies, and dark-web researchers consistently classify Red Rooms as hoaxes for several reasons:

- Streaming live video on the dark web is extremely difficult due to slow network speeds.
- Such an operation would be impossible to hide from global law enforcement.
- Verified dark-web criminal markets do not host or advertise anything like this.
- Most "Red Room links" are scams designed to steal money.

Hitmen for Hire

The dark web contains marketplaces where you can hire a professional “hitman” to harm or kill someone. These sites often claim:

- “Professional assassins for hire”
- Payment through Bitcoin or Monero
- Guaranteed anonymity
- Menu-style pricing for different crimes

There has never been any verified case of a legitimate murder-for-hire marketplace operating on Tor.
Cybersecurity experts and law enforcement agree:

- Every “hitman site” is designed to steal cryptocurrency.
- None of them deliver what they claim.
- Operators disappear after taking payment.
- Many sites reuse the same text, images, and fake “testimonials.”

I think maybe the law is lying

Secure Drop

- Edward Snowden
- NYT, Guardian, Washington Post

- Used for
- whistleblowing,
- journalism,
- scenario where someone wants to share information without revealing their identity

A platform designed to allow people to submit sensitive or confidential information securely and anonymously.

Secure drop is for
Confidentiality
Anonymity
End-to-End Security

Functionality — Fingerprinting and metadata

Screen size resolution stays the same

- to reduce likely hood of fingerprinting tor makes all the browsers identical configured to block things like Flash, JavaScript.
- Browser resolution identical so you can't be tracked, because people can track you if you have a different resolution as every has the same.

Fonts

- Configured to show that everyone's fonts look the same to prevent finger prints

Ads

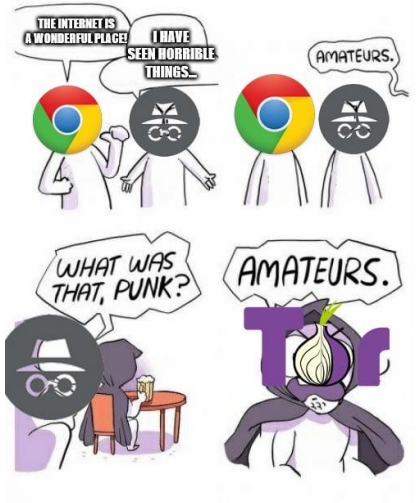
- Tor actively blocks of ads and rejects third party cookies, because Ads can still track you in a certain way Tor just limits the tracking

DNS

- Tor browsers specifically routes DNS queries through TOR so any DNS requests gets sent through TIR

Ip headers

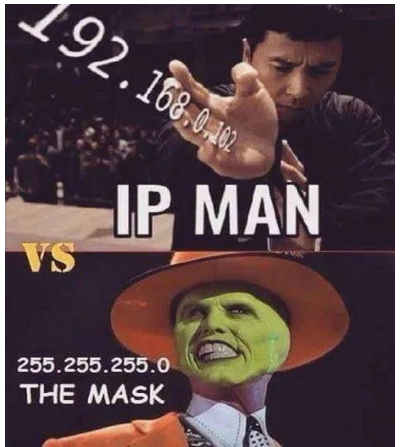
- Ip headers are anonymized , so no leaks occur , Disable **WebRTC** and **local DNS** on your system to further reduce the risk of IP leakage.



.onion sites

- Servers IP is never revealed
  - It connects to the TOR network, not the open internet. This prevents DDoS attacks and physical location tracking.
- The onion address is a hash of the public key

- Server makes an outbound connection to Tor, it works behind firewalls and NATs without requiring open ports



PGP with Cleopatra

- Task: Create and decrypt keys via linux and mobile
- Setup:
- Install openkeychain or IPGmail
- Download cleopatra from VM
- Export key from PC
- Import to mobile
- Verify and sign messages
- Cleopatra is installed using the command: sudo apt install kleopatra gnupg2

TOR Setup

- TOR is available for download on mobile devices as TOR Ornet

Cryptography

- The practice and study of techniques used to secure information systems.
- Encryption – converting plaintext into ciphertext using algorithms
- Decryption – reverse process of turning ciphertext to plaintext
- Algorithm – a step by step procedure used to solve a problem using inputs and outputs

Cryptography is vital in SOC as it reinforces CIA values. It protects confidentiality by encrypting sensitive data, ensures integrity by hashing and supports availability by enabling the correct authorization to the correct users.

Types of Cryptography

- Symmetric: uses one key for encryption and decryption
- Asymmetric: uses a public key to encrypt and a private key to decrypt
- Digital signature: is used to prove authencity and integrity using public and private keys to sign and verify
- Certificates: documents used to prove identity by linking a public key
- Public key: is a commonly shared key
- Private key: a key that is not shared

Tasks

- SHA – 1
- SHA – 256
- MD5
- MD6
- DES

Using the following encryption, decryption and hashing tools create and compare the differences in methods via the software that is used.

Stenography

- Stenography is the practice of concealing information. It involves hiding data within ordinary files and messages to prevent detection and can be extracted on the receiving end it is used to conceal any digital data often paired with encryption
- Algorithms:
- AES- Advanced Encryption Standard is the most used symmetric encryption algorithm
- RSA - Rivest-Shamir-Adleman is a popular public key algorithm used for digital certificates and TLS/SSL
- ECC - Elliptic Curve Cryptography provides strong encryption with smaller keys often used for IOT
- SHA – Secure Hash Algorithm is used for data integrity and digital signatures
- Blowfish & Twofish is a symmetric algorithm offering fast performance

TOR Tools


Dark Web Tools
TOR Browser
Web browser
Ahmia
Search engine
HayStack
Search engine
Tor66
Search engine
Torch
Search engine
Onion Engine
Search engine
Telemetry
Telegram search
Library of Leaks
Leaks & breaches
HavelbeenPwned
Search data breaches
DeHashed
Search data breaches
LeakOSINT
Telegram bot
UniversalSearchBot
Telegram bot
DeepDarkCTI
Collection of CTI sources
DarkwebDaily.Live
Links to onion sites
Onion.live
Links to onion sites
Tor.link
Links to onion sites
The Hidden Wiki
Links to onion sites
TorCrawl.py
Crawl and extract webpages
Aleph
Search data on the Dark web
TOR2web
Access to Tor hidden services
PGP Tool
Encrypt, decrypt, and verificate PGP