

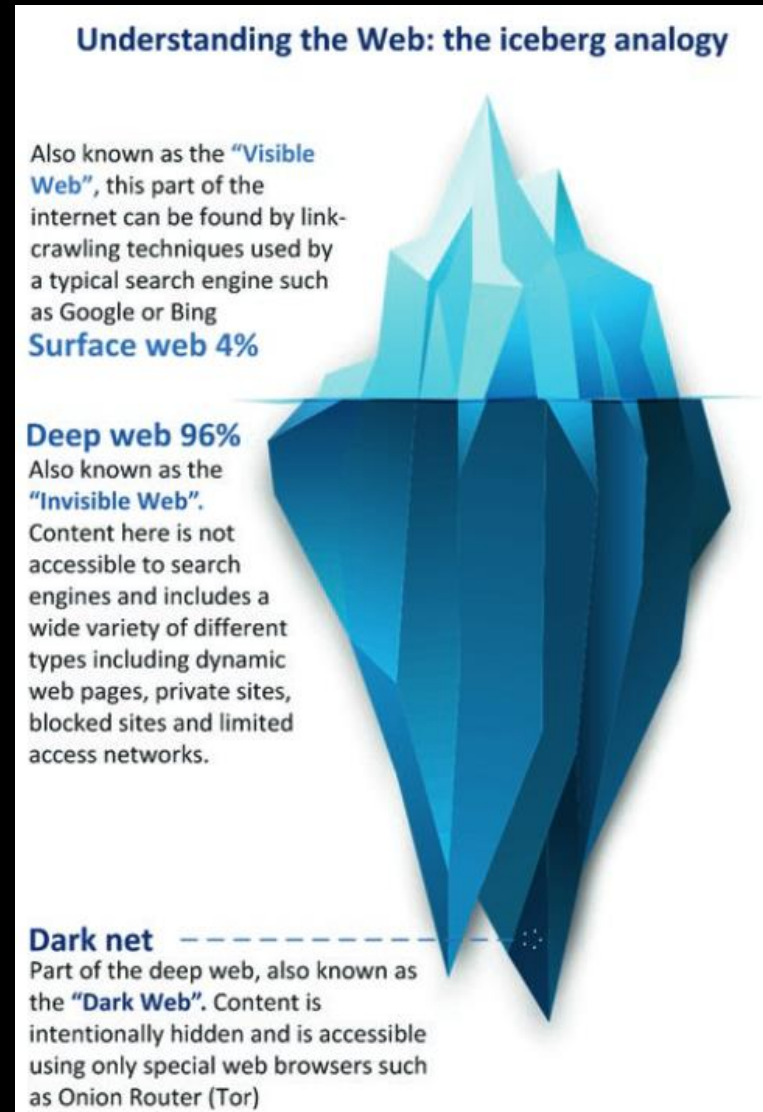
MCAST



**HackSpace**

Demystifying the Dark Web

# Introduction



(EMCDDA–Europol, 2016)

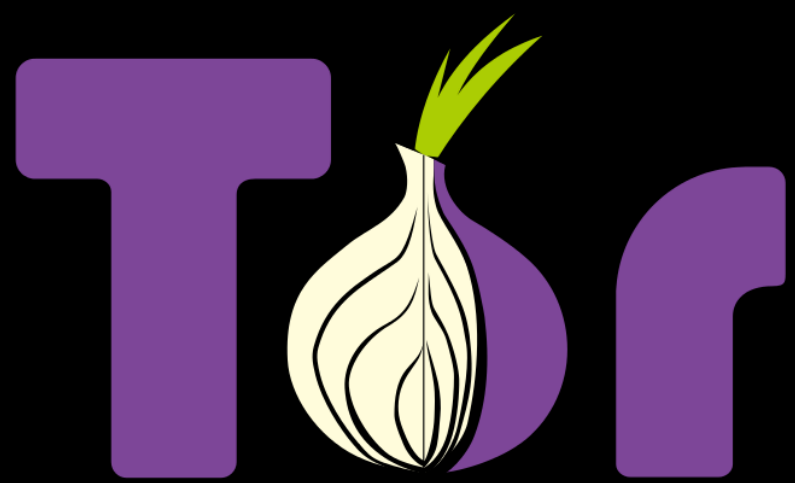
# Dark Web Users

- Journalists
- People in countries facing censorship
- Criminals (cybercriminals, drug/arms dealers etc)
- Whistleblowers
- Privacy-minded people

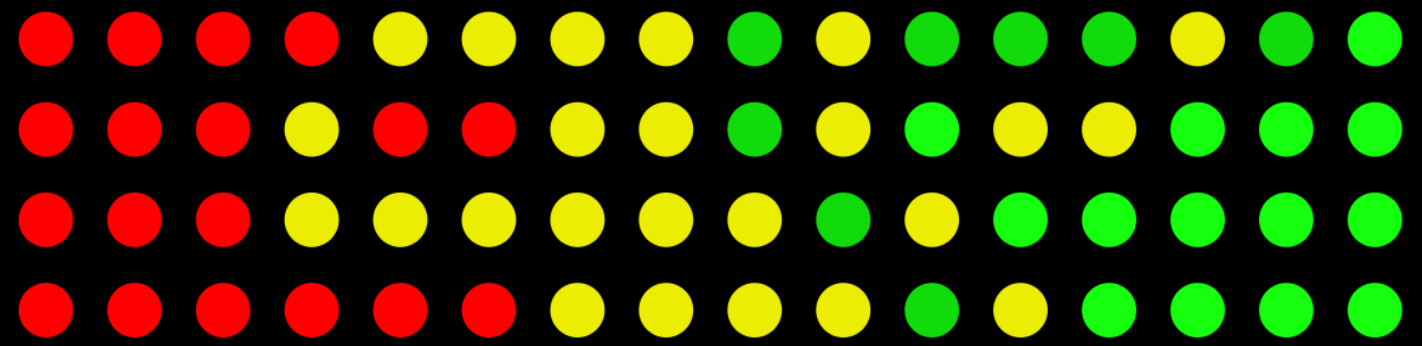
# Services on the Dark Web

- Anonymous browsing
- Anonymous messaging
- Anonymous file-sharing
- Forums (very good source of intelligence for threat hunters)
- Marketplaces

# Infrastructure



I2P



# Disclaimer

- Sites on the dark web might contain offensive, disturbing and illegal content.
- Do not trust any downloaded files (this should also apply to the surface web, anyway).
- Always use a VPN service to access the dark web.

# Freenet

- Can be regarded as a distributed file sharing network.
- Lets you to anonymously share files and browse freesites.
- Users contribute by allocating some of their storage for the parts of files in the network. You cannot know what you are actually storing!
- Communication is encrypted and traffic is routed through outer nodes. This makes tracking the source of the communication extremely difficult.

# Freenet

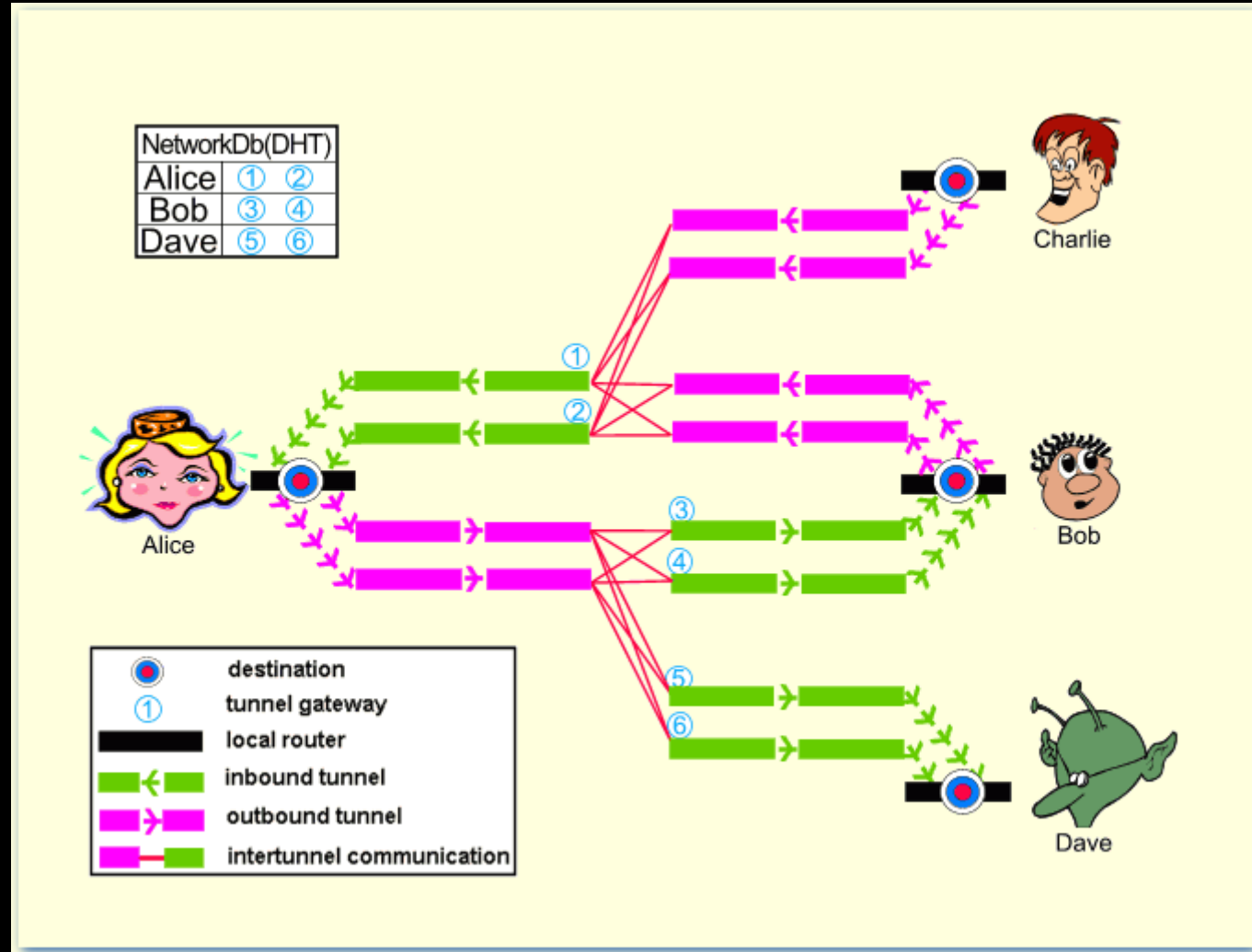
## DEMO: Connecting to Freenet



# I2P

- I2P is an overlay network that uses multiple layers of encryption to anonymise traffic.
- Its main goal is to protect communication from eavesdropping.

# I2P



# I2P

## DEMO: Connecting to I2P

# The Onion Router (TOR)

- TOR is the most popular network to access the dark web.
- Like most things in life, it used and abused.
- TOR hidden services are only accessible within the TOR network.
- TOR users can also browse the internet while hiding their public IP address from the websites they visit.

# The Onion Router (TOR)

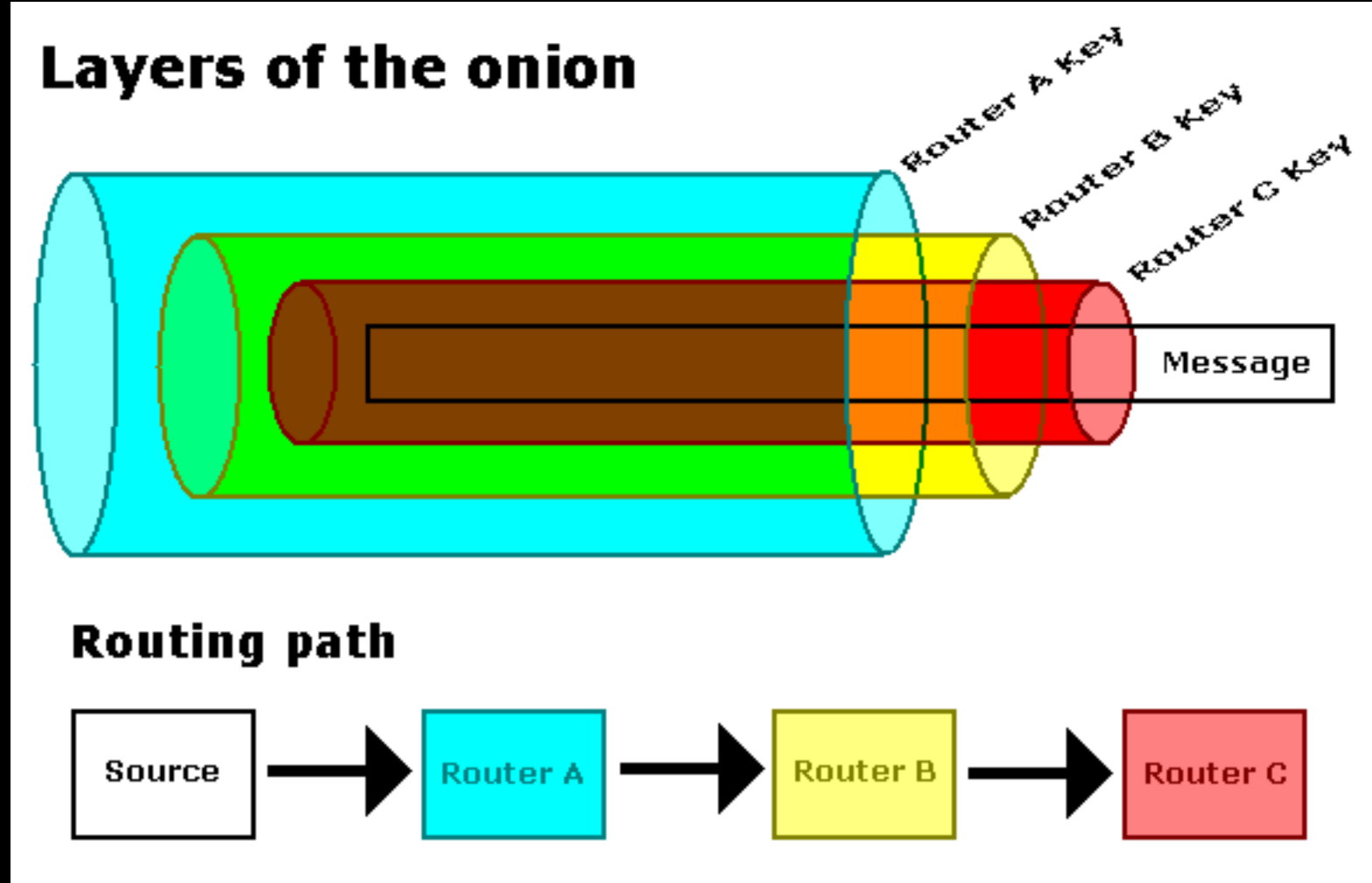


<https://pixabay.com/photos/onion-vegetable-sliced-red-onion-6676931/>

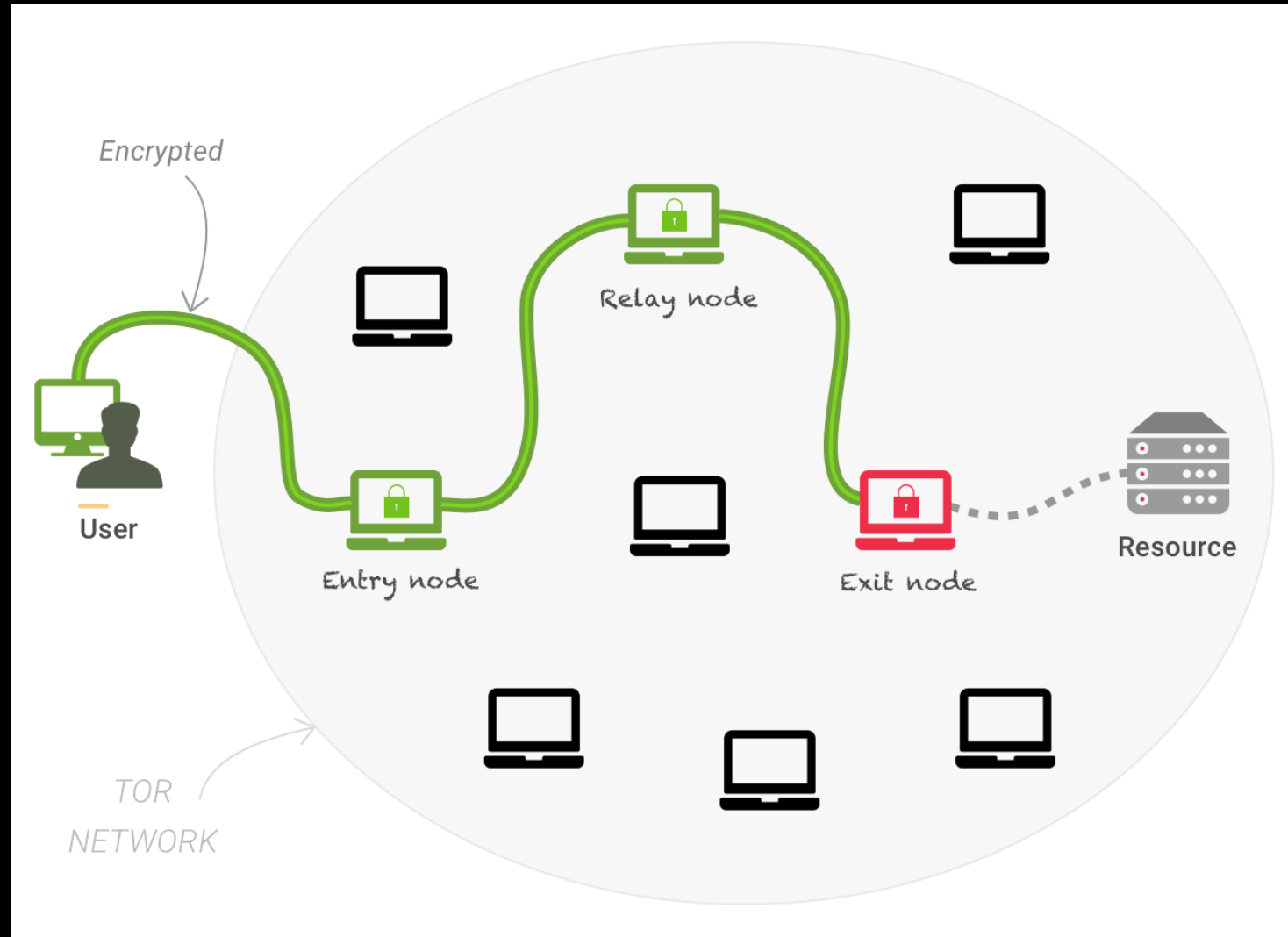
# The Onion Router (TOR)

DEMO: Understanding TOR Operation

# The Onion Router (TOR)



# The Onion Router (TOR)



<https://devopedia.org/tor-network>



# The Onion Router (TOR)

DEMO: Using TOR Browser

# Honey TOR Nodes



## **HOnions: Towards Detection and Identification of Misbehaving Tor HSDirs**

Amirali Sanatinia  
Northeastern University  
amirali@ccs.neu.edu

Guevara Noubir  
Northeastern University  
noubir@ccs.neu.edu

DEF CON 24 - Guevara Noubir, Amirali Sanatinia - Exposing Snooping Tor HSDirs

# Finding Hidden TOR Services

## Hunchly Daily Dark Web Report

Finding good investigation targets on the dark web can be a tricky task and many investigators find the dark web to be a scary place.

Our daily dark web reports can help you identify new hidden services, or find investigation targets that you might not otherwise know about. It is 100% free and every day you will receive a link to a spreadsheet you can download or view online.

Email \*

☐ Notify me when Hunchly publishes new blog posts or hosts OSINT webinars.

Send Me Reports

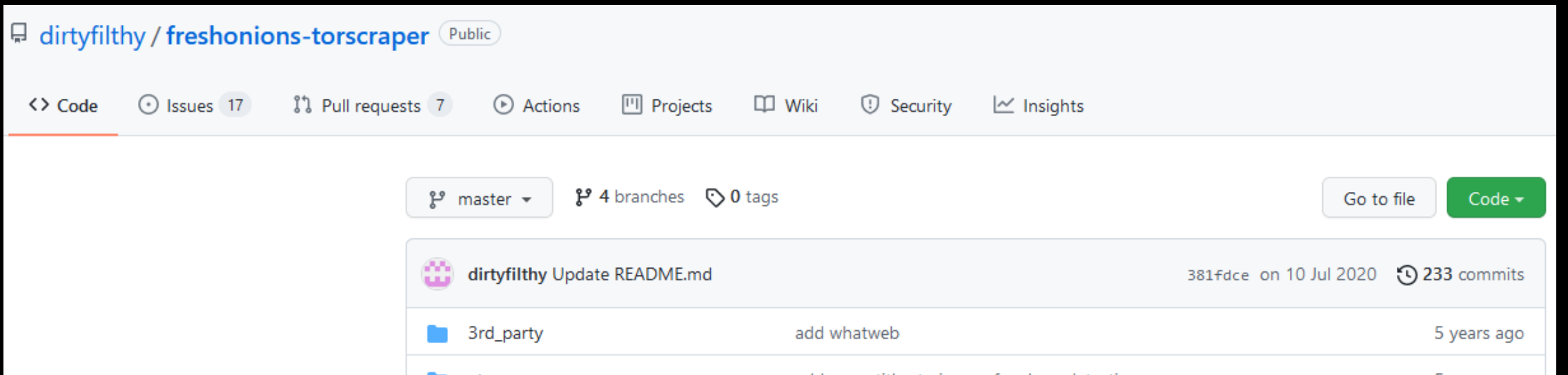
WARNING! We are not analyzing the hidden services for content. The hidden service addresses you receive could contain links to drug markets, child pornography, malware or more benign things like pictures of cats. Use your own discretion, and your common sense.

If you do discover child pornography please report it to the National Center for Exploited and Missing Children by clicking [here](#).

# Finding Hidden TOR Services

DEMO: Using Hunchly Reports

# Finding Hidden TOR Services



# Finding Hidden TOR Services

DEMO: Using Fresh Onion

# Hidden Service URL

- Version 2: 16 bytes ending with .onion
- Version 3: 56 bytes ending with .onion
- Generation of addresses involves cryptographic calculations. We might be able to delve into this in a future talk 😊.

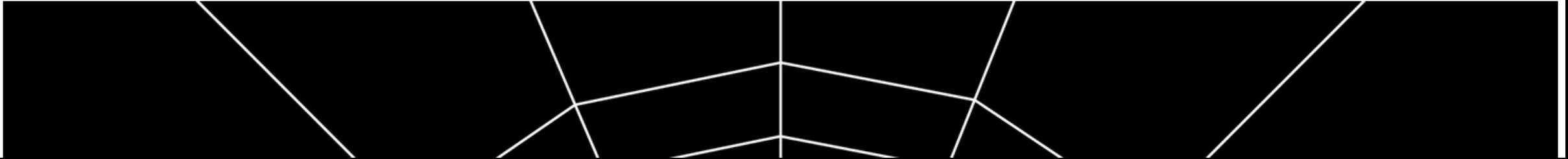
# Case Studies - Hansa Marketplace

ANDY GREENBERG

SECURITY 03.08.2018 11:38 AM

## Operation Bayonet: Inside the Sting That Hijacked an Entire Dark Web Drug Market

Dutch police detail for the first time how they secretly hijacked Hansa, Europe's most popular dark web market.






# Case Studies - Matthew Falder

## Matthew Falder: How global taskforce caught Birmingham paedophile

By Jessica Labhart  
BBC News

🕒 19 February 2018

# Case Studies - Ransomware

  
**DarkFeed**  
DeepWeb Intelligence Feed

Have a new onion? send us on [Red-Alert](#)

Updated [every day!](#)

**Use this page for research purposes only**, the link route through Deep2Web Proxys if you got a problem just copy onion URL to TOR

**BTC Donations :** [bc1qm3cxecf5jetsrmqg95pla4cjr0j8s0sxhvm8e2](#)

[Home](#) [RansoMonitor](#) [RansomWiki](#) [Threat Intelligence](#) [About](#)

Search:

Name	↕ Tor/Cleartnet ↕	Link ↕	Description ↕	RansomWare Note ↕	Decryptor ↕	Status ↕
Conti News	TOR	<a href="#">Link</a>	Blog Website	<a href="#">View</a>	Unavailable	UP
Hive Leaks	TOR	<a href="#">Link</a>	Blog Website	<a href="#">View</a>	Unavailable	UP
LOCKBIT 2.0	TOR	<a href="#">Link</a>	Blog Website	<a href="#">View</a>	Unavailable	UP
Corporate Leaks	TOR	<a href="#">Link</a>	Blog Website	None	Unavailable	UP
Pysa	TOR	<a href="#">Link</a>	Blog Website	<a href="#">View</a>	Unavailable	UP
SunCrypts	TOR	<a href="#">Link</a>	Blog Website	<a href="#">View</a>	Unavailable	UP
Everest	TOR	<a href="#">Link</a>	Blog Website	<a href="#">View</a>	Unavailable	UP
Dopple Leaks	TOR	<a href="#">Link</a>	Blog Website	<a href="#">View</a>	Unavailable	UP
Cuba	TOR	<a href="#">Link</a>	Blog Website	<a href="#">View</a>	Unavailable	UP