

Penerapan **OSINT** Dalam **DARK WEB**

21+





DARKNET

DISCLAIMER

- **PERHATIAN !!!** Dark Web penuh dengan konten kriminal, kejahatan, kekerasan, dan perbuatan tidak etis yang sangat mengganggu.
- Kami melarang anda untuk melakukan transaksi apapun yang ada di halaman Dark Web/Net.
- Segala jenis informasi yang disampaikan pada Webinar/rekaman Webinar ini adalah untuk tujuan pendidikan dan menambah pengetahuan/wawasan semata bukan untuk mendukung aksi kejahatan dan/atau perbuatan yang dapat merugikan pihak lain.
- Dengan mengikuti Webinar/menonton rekaman webinar ini anda menyetujui bahwa setiap hal/tindakan terlarang yang anda lakukan maka hal/tindakan terlarang tersebut tidak berhubungan sama sekali dengan Orang Siber Indonesia.

The screenshot shows a YouTube channel page. At the top, the URL is youtube.com/c/OrangSiber/featured. The channel name 'orang siber indonesia' is displayed in the search bar. The main video thumbnail features a blue and white graphic with the text 'ORANGSIBER'. Below the thumbnail, the channel name 'Orang Siber' is shown with 867 subscribers. A 'SUBSCRIBED' button with a bell icon is visible. The navigation bar includes links for HOME, VIDEOS, PLAYLISTS, CHANNELS, DISCUSSION, and ABOUT. On the left, a sidebar shows links for Home, Trending, Subscriptions, and Library.

Please Like, Subscribe & Share
Channel Youtube Orang Siber Indonesia
<https://www.youtube.com/c/OrangSiber>

Who Am I ??

Contact me : @camorra_13

Supported by : @EnamnyaTigaKali

Where you can find us:
https://t.me/OSINT_ID



Pengertian



SURFACE WEB/NET

Bagian dari internet yg tersedia utk publik & dapat dicari dgn mesin pencarian Web standar



DEEP WEB

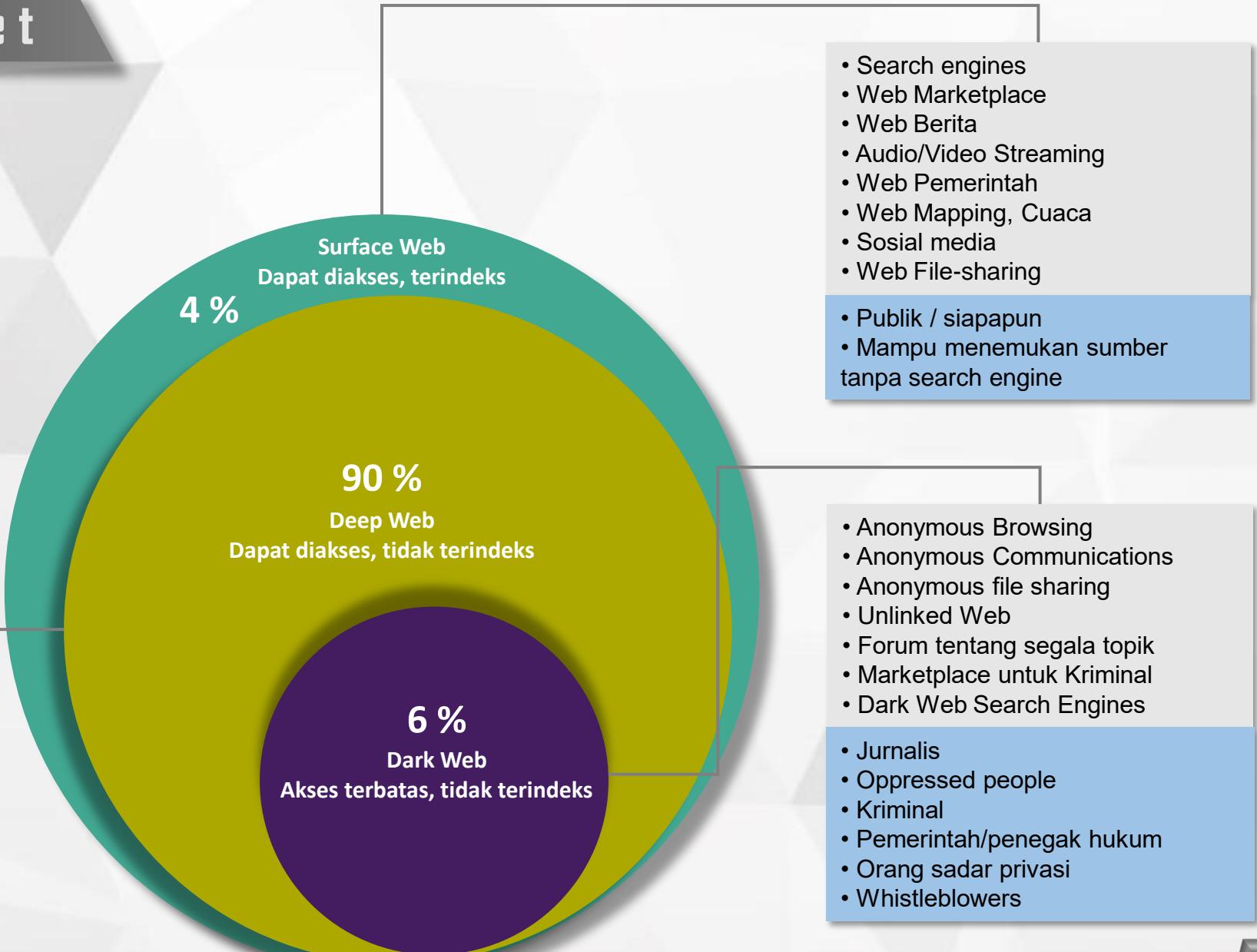
Bagian dari internet yang isinya tidak terindeks oleh mesin pencarian web standar



DARK WEB/NET

Bagian dr internet yg tdk terindeks oleh mesin pencarian Web standar & utk mengaksesnya hrs gunakan suatu jaringan Internet yg memerlukan software, konfigurasi, dan otorisasi tertentu

Level of Internet

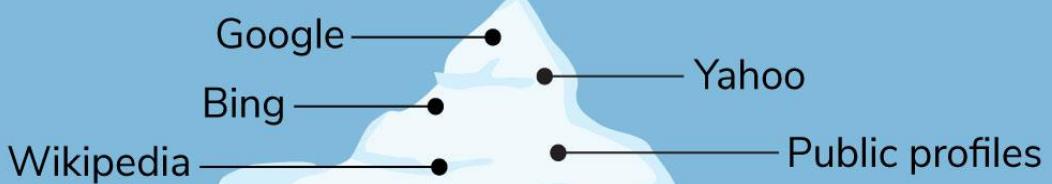


Level of Internet

4%

Surface Web

Indexed and easily searchable.



90%

Deep Web

Not indexed, tougher to find.



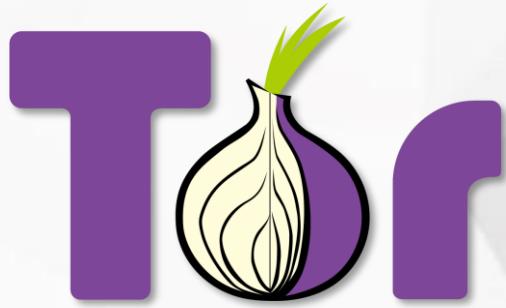
6%

Dark Web

Obscured, difficult to discover.



Dark Web Access



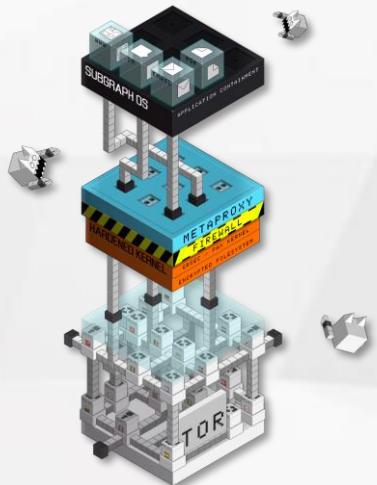
TOR Browser



Invisible Internet Project (I2P)



Freenet



Subgraph OS

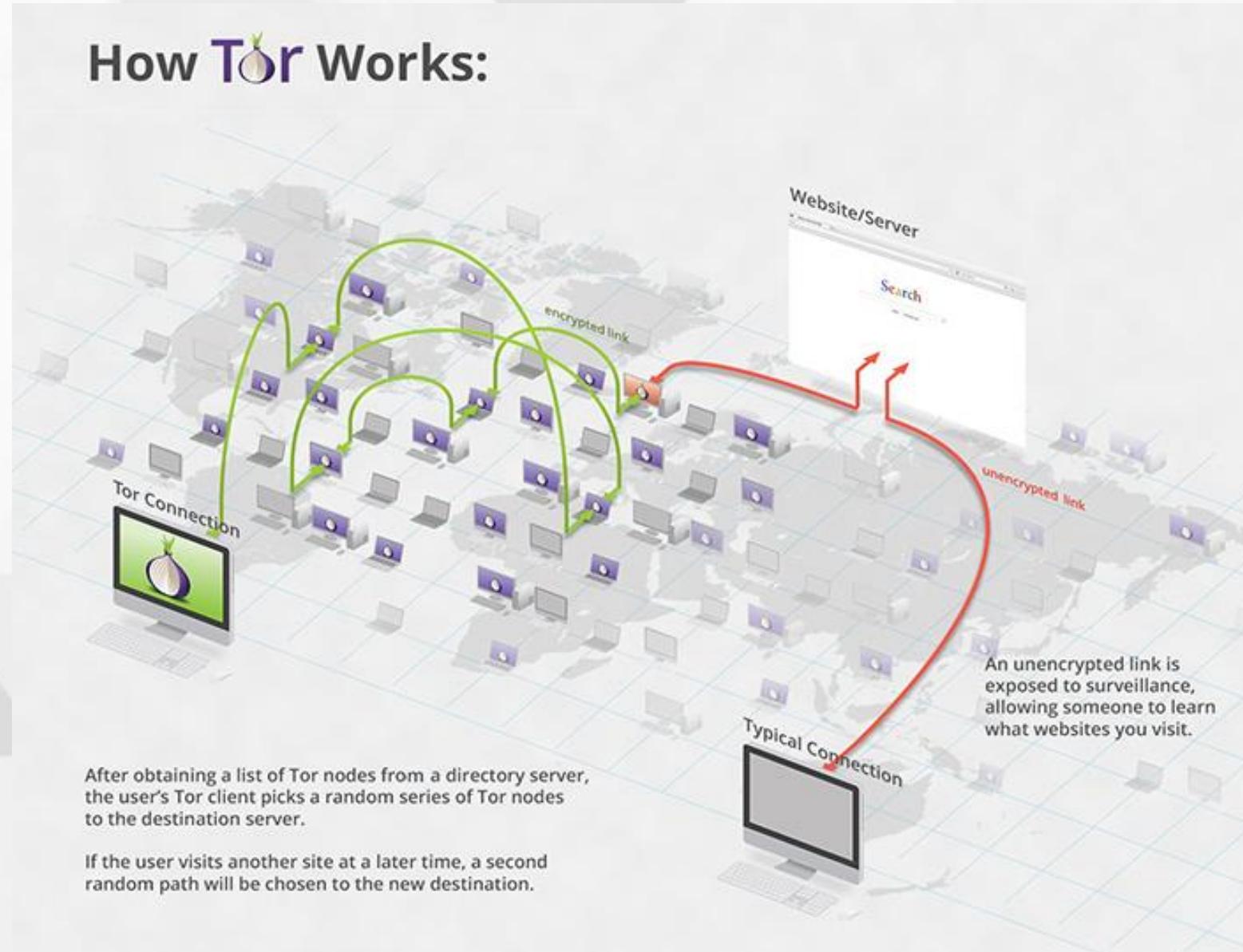


The Amnesic Incognito Live System



Whonix

Ilustrasi TOR



TOR mengarahkan lalu lintas Internet melalui lebih dari 7000 relay jaringan (TOR Nodes) yang dibuat oleh sukarelawan secara gratis untuk menyembunyikan lokasi & penggunanya dari siapa pun

TOR Snooping

Researchers find more than 100 Tor nodes that are snooping on users

By Ryan Whitwam on July 27, 2016 at 10:00 am | [10 Comments](#)

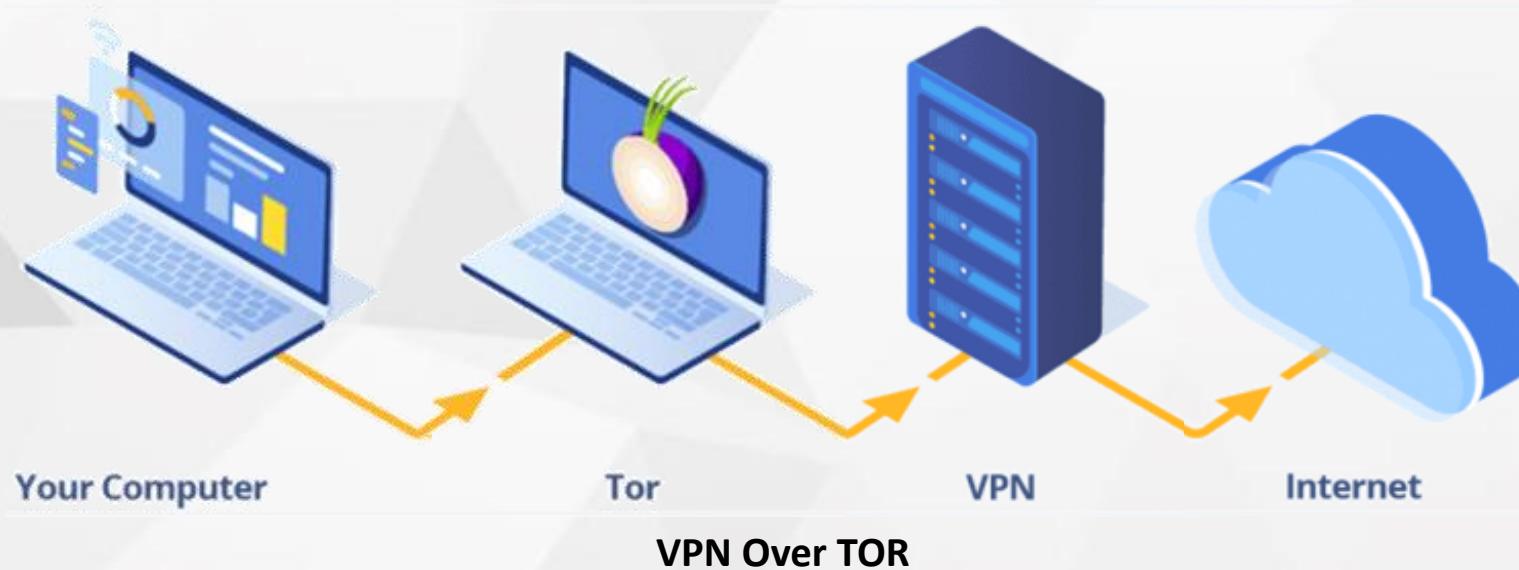
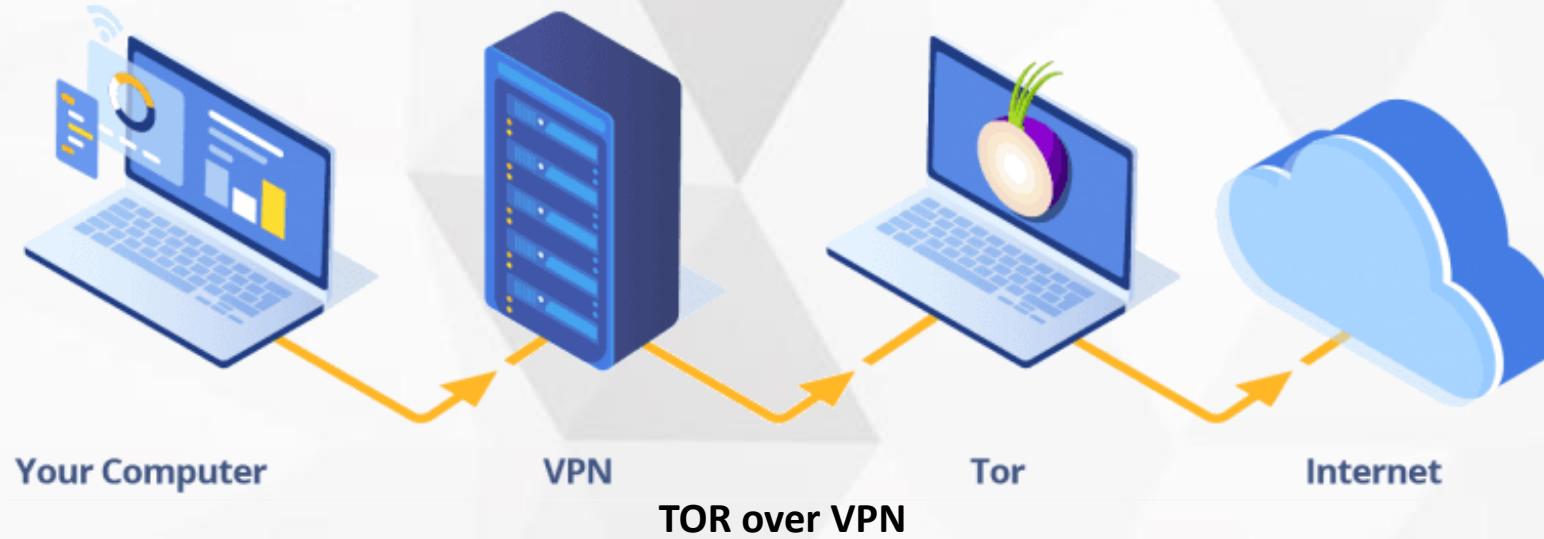


Tor, or "The Onion Router" as it was originally known, is used around the world as an anonymity network. It provides a private method of communication for journalists, those living under authoritarian governments, and people who are just up to some shady stuff. While [Tor](#) is still the most robust form of online anonymity we have, it's not bulletproof as the repeated takedown of [The Silk Road](#) and other law enforcement actions have shown. Now, two computer scientists say they've uncovered snoops inside the Tor network that may be listening in on what you're doing.

Bagaimana untuk menghindari pengintai pada TOR Nodes ?



VPN + TOR



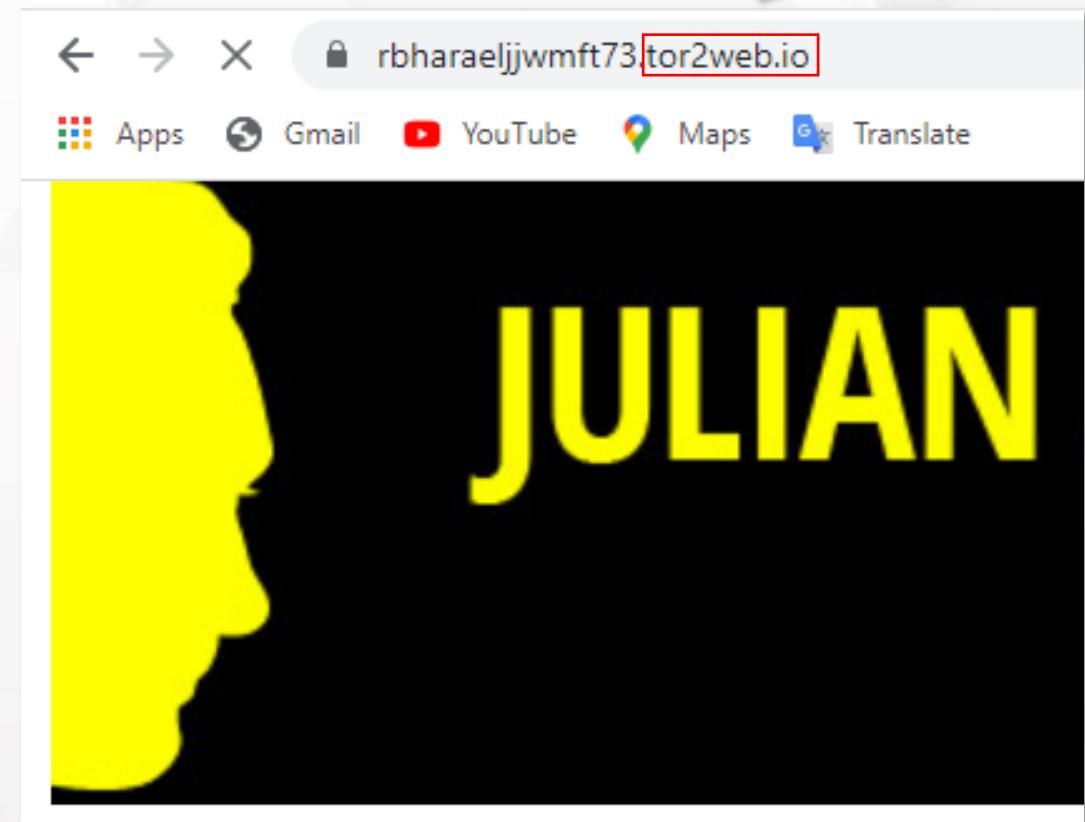
Menggunakan TOR over VPN / VPN over TOR adalah cara untuk menambahkan security layer. VPN melindungi Anda jika jaringan TOR disusupi sehingga itu dapat membantu untuk menyembunyikan identitas pengguna TOR

Dark Web Address



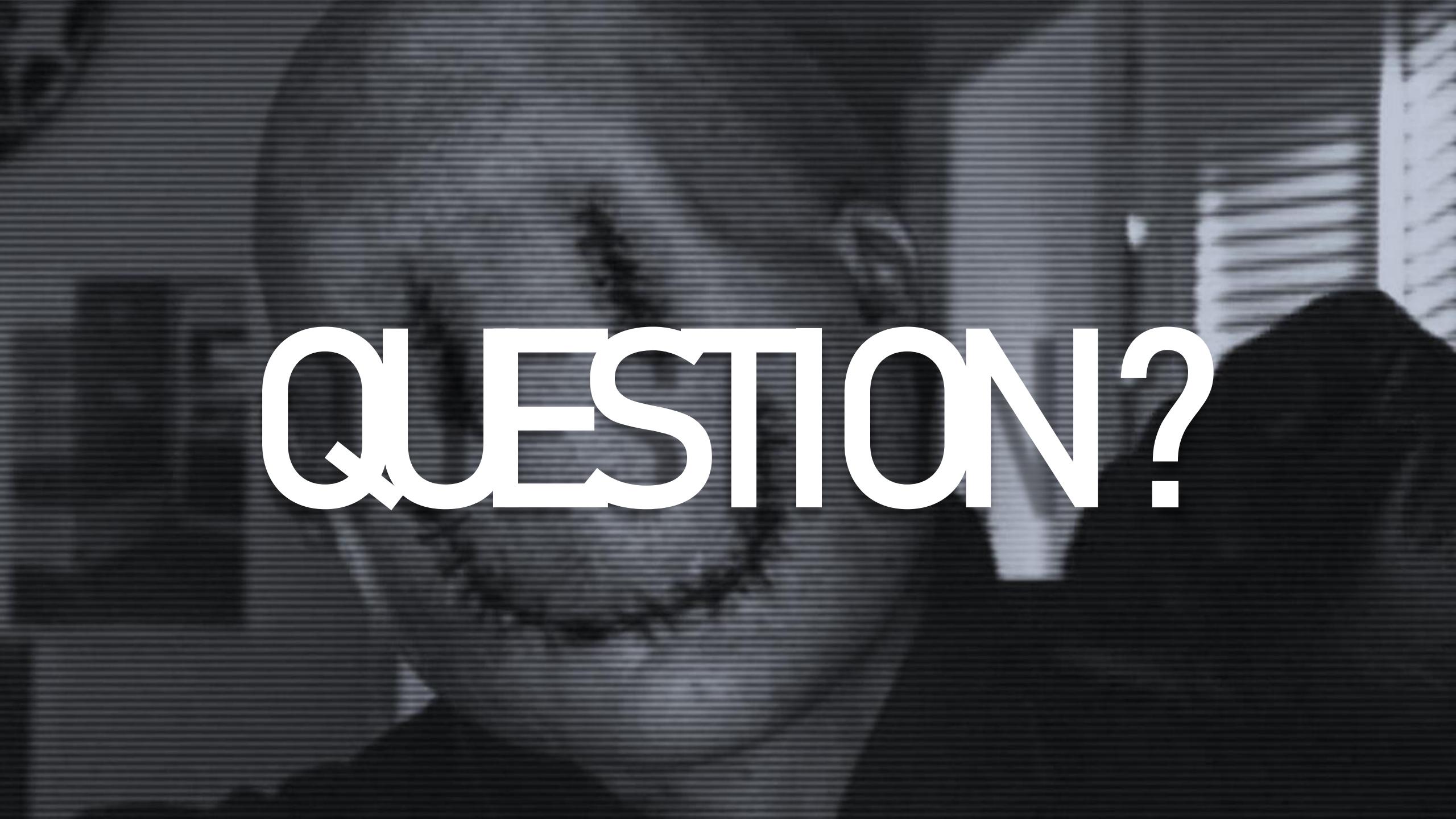
Matikan JavaScript, Flash dan Java, TOR tidak dapat melindungi data anda dengan konten aktif seperti JavaScript, Adobe Flash, Java, QuickTime, ActiveX controls, VBScripts, dll. Karena aplikasi binary ini berjalan dengan user account's privileges anda dan sangat mungkin dapat mengakses dan membagikan data anda

Ingin membuka TOR Site via Non Tor Browser ?



Just if its ok to lose your anonymity...

<https://www.tor2web.org>

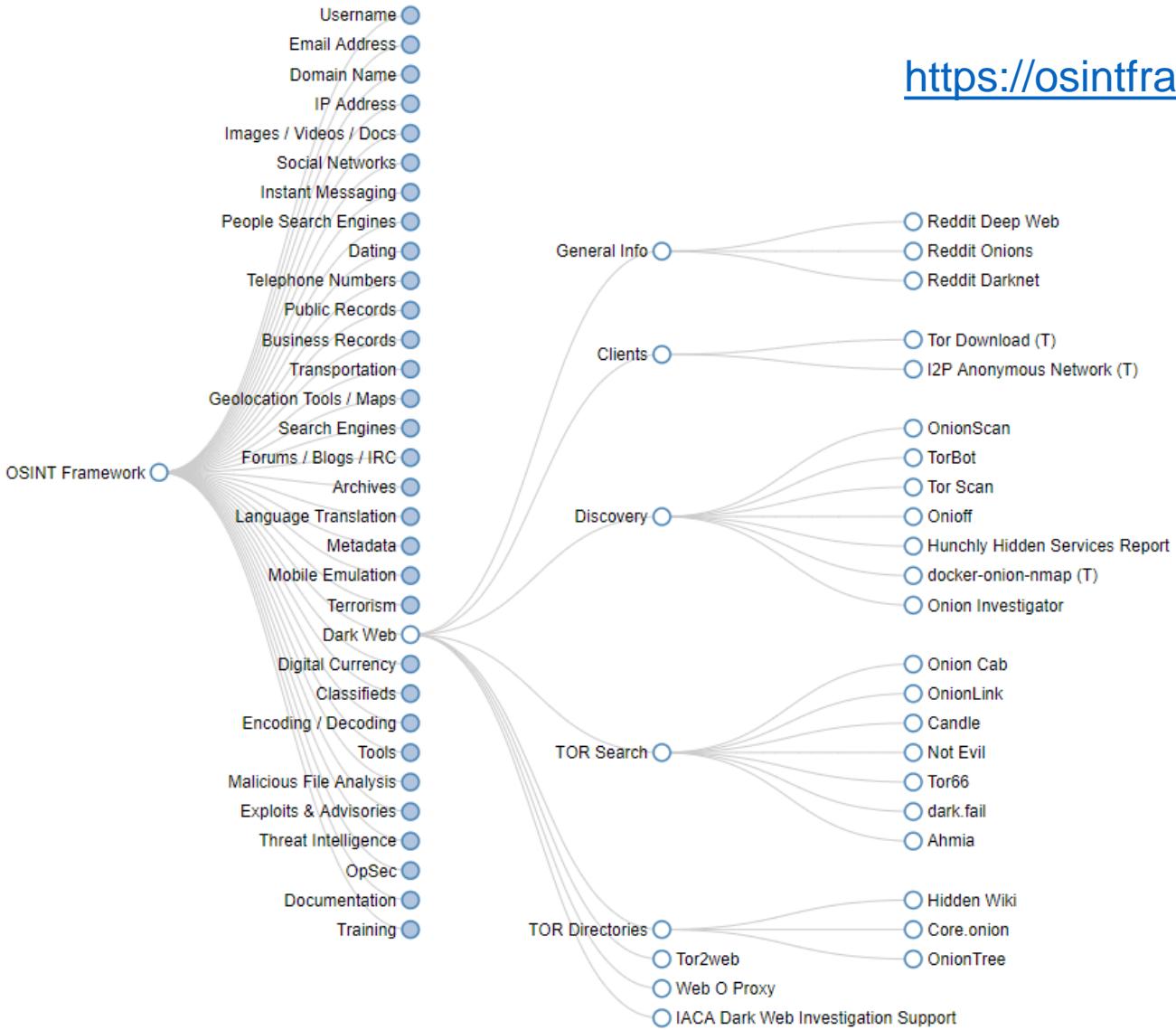


QUESTION?

Mengapa OSINT Analyst perlu mengunjungi Dark Web ??

- Rasa keingintahuan / curiosity
- Melindungi komunikasi
- Untuk menganonimkan traffic /aktivitas mereka
- Menjejaki aktivitas target
- Melacak penipuan finansial / crypto currency
- Membantu penegak hukum / intelijen

OSINT Framework



<https://osintframework.com/>

Deep Web Search Engine



- <https://www.yippy.com> — A metasearch engine that combines the results of several top search engines.
- <https://archive.org/index.php> — A database of tens of thousands of movies, live music, audio, texts, and home of the Wayback Machine that allows you to find old versions of web pages, over 55 billion.
- <http://www.directsearch.net> — A list of hundreds of specialty databases and search engines. No longer maintained, but still perhaps the most complete list of the deep web.
- <http://vlib.org> — Started by none other than Tim Berners-Lee, the VLib is not the biggest index of the Web, but it is one of the highest-quality.

Dark Web Search Engine



- Ahmia <http://msydqstlz2kzerdg.onion>
- Excavator
<https://2fd6cemt4gmccflhm6imvdfvli3nf7zn6rfrwpsy7uhxrgbypwf5fad.onion.ly/>
- Not Evil <http://hss3uro2hsxfogfq.onion>
- Hidden Wiki
http://zqktlwiuavvvqqt4ybvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbym2qad.onion/wiki/index.php/Main_Page
- Duck Duck Go <https://3g2upl4pq6kufc4m.onion>
- Candle <http://gjobqjj7wyczfqie.onion>
- SearX <http://ulrn6sryqaifefld.onion>
- Facebook <https://www.facebookcorewwi.onion>
- Bitcoin & Other Cryptocurrency <http://ow24et3tetp6tvmk.onion>
- BBC Tor Mirror <http://bbcnewsv2vjtpuy.onion>
- Hidden Answers <http://answerstedhctbek.onion>
- Secure Drop:
 - Forbes: <http://t5pv5o4t6jyjilp6.onion>
 - The Financial Times: <http://xdm7flvwt3uvrrd.onion>
 - Reuters: <http://smb7p276iht3i2fj.onion>
- ProtonMail <https://protonirockerxow.onion>
- Secmail <http://secmailw453j7piv.onion>
- Raptor <http://raptortiabg7uyez.onion>



GitHub

- <https://github.com/saeeddhqan/Maryam> — OWASP Maryam is an Open-source intelligence(OSINT) and Web-based Footprinting optional/modular framework based on the Recon-ng core and written in Python.
- <https://github.com/DedSecInside/TorBot> — Open Source Intelligence Tool for the Dark Web.
- <https://github.com/dirtyfilthy/freshonions-torscraper> — This is a copy of the source for the http://zlal32teyptf4tvi.onion hidden service, which implements a tor hidden service crawler / spider and web site.
- <https://github.com/k4m4/onioff> — A simple tool - written in pure python - for inspecting Deep Web URLs (or onions).
- <https://github.com/MikeMeliz/TorCrawl.py> — TorCrawl.py is a python script to crawl and extract (regular or onion) webpages through TOR network.



QUESTION?
Prepare for Live Demo

Live Demo

The screenshot shows a web browser displaying the Hunchly website at hunch.ly/darkweb-osint/. The page has a blue header with the Hunchly logo (a cartoon character wearing a fedora) and navigation links for Your Industry, Pricing, Resources, Blog, Support, Contact, and a prominent 'Get Hunchly Now!' button. Below the header, a large blue banner features the text 'Hunchly Daily Dark Web Report'. The main content area explains that finding investigation targets on the dark web can be tricky and introduces the daily dark web reports. It states that these reports help identify new hidden services and provide a free spreadsheet download or online view. A form for entering an email address is present, along with a checkbox for notifications and an orange 'Send Me Reports' button. A warning at the bottom cautions users about the nature of hidden service addresses.

hunch.ly/darkweb-osint/

Gmail YouTube Maps Translate

 **HUNCHLY**

Your Industry ▾ Pricing Resources Blog Support Contact Get Hunchly Now!

 **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 *

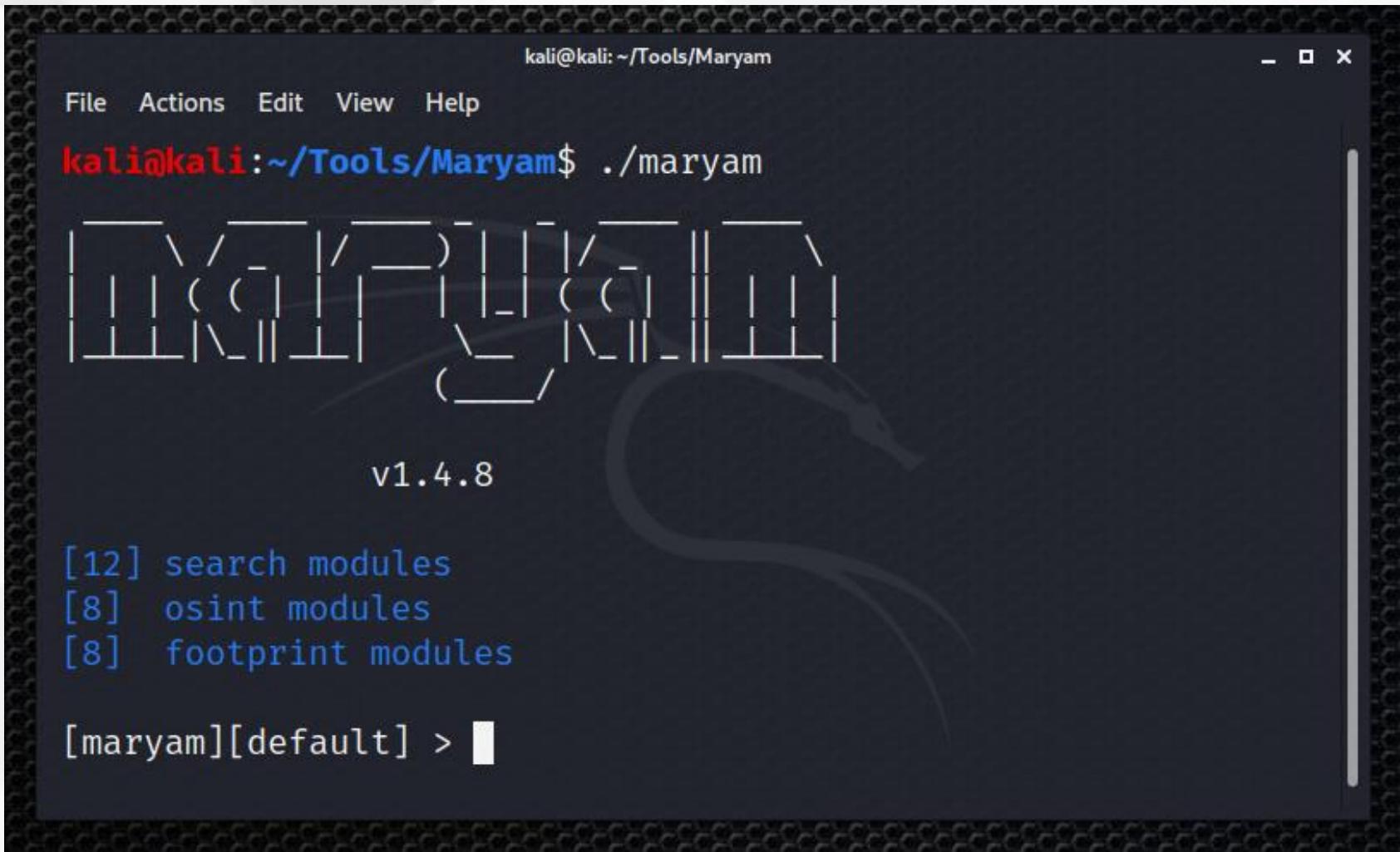
Notify me when Hunchly publishes new blog posts or hosts OSINT webinars.

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.

<https://www.hunch.ly/darkweb-osint/>

Live Demo



kali@kali:~/Tools/Maryam

File Actions Edit View Help

kali@kali:~/Tools/Maryam\$./maryam

v1.4.8

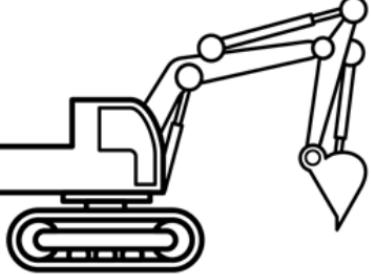
[12] search modules
[8] osint modules
[8] footprint modules

[maryam][default] > █

<https://github.com/saeeddhqan/Maryam>

Live Demo

C https://2fd6cemt4gmccflhm6imvdfvli3nf7zn6rfrwpsy7uhxrgbypvwf5fad.onion.ly 140% ... ☆



EXCAVATOR

"No javascript. Safe search. We don't track you."

Enter your request

SEARCH

ADVERTISE | ADD URL | ABOUT
EXCAVATOR © 2019 - 2020

<https://2fd6cemt4gmccflhm6imvdfvli3nf7zn6rfrwpsy7uhxrgbypvwf5fad.onion.ly>

Dark Market

MARKET URLs	
Dark Market	darknet3ysxpbjtvbyqorzuq3bp4pk3vt4fuhqxz6h2bzj2kyjbisqd.onion/signup/N07TG8
ToRReZ Market	f3dxwzcmojrlpvehqwcecwe3amg6rkzgilcn4xqxmaiezoedjf6rtid.onion/register/JnIG
DarkOde Reborn	darkoddrkj3gqz7ke7nyfk7o72hlvr44uz5zl2xrapna4tribuorqd.onion/welcome/RDKbK303437545709z
Neptune Market	neptunes72him6enh2s2x3btm45fhwnqwwmndig44ctewvyjoqmd5eyd.onion/user/register.html?ref=2466-a154c
Agartha Market	agarthaourmnyhq3.onion/register/4387269541
White House	auzbdiguv5qtp37xoma3n4xfch62duxtdio4cfrrwbxgckipd4aktxid.onion
Monopoly	monopolyberbucxu.onion
Cannazon	cannazon4gbjluus.onion
The Majestic Garden	garden2b7zwrjskh2y3f4pkscgg2waogjp2ilax2mvikjlzmamylznad.onion
Invictus Market	invicus3w24e22upa4scshje3e5rxqjjv4hf7l7p6lckzkukylsewwid.onion
Versus Project	pqqmr3p3tppwqvavapi6fa7jowrehgd36ct6lzc26qqormaqvh6gt4jyd.onion
Yellow Brick	ck73ugjvx5a4wkhsmrfvwhlrq7evceovbsb7tvaxilpahybdokbyqcqd.onion
Silk Road 4	silkroadxjzvoxyh.onion
Big Blue	c4mqr4cam4rgl7hxoinhlczlws26n5hm5yq6uoijqiz2ejrnvhypqd.onion
Vice City	vice2e3gr3pmakukidllstulxvb7a247gkguihzyk3gqwdpolqead.onion

<https://marketurls.org>

Case Example

Armory Guns

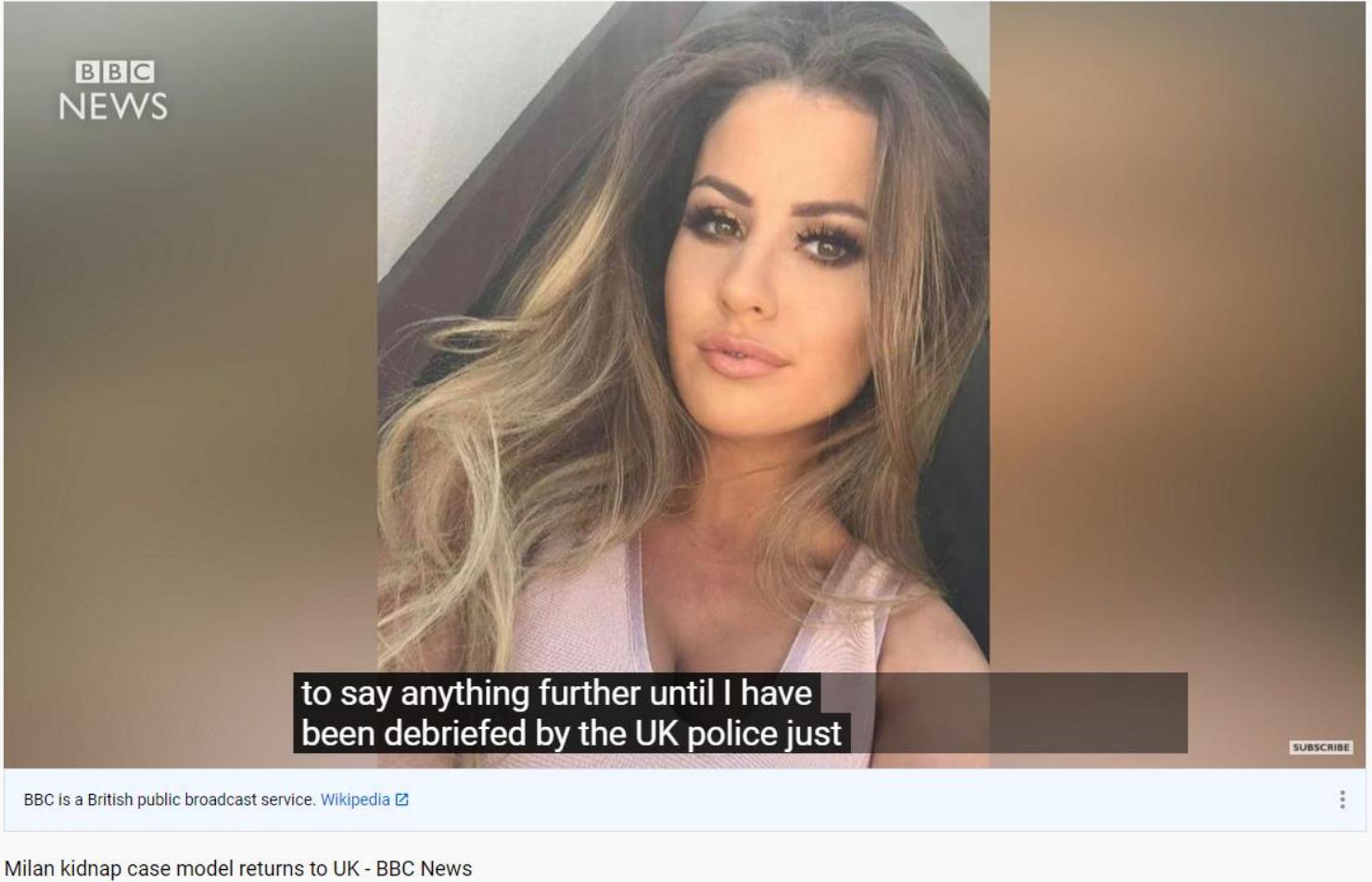
5xxqhn7qbtug7cag.onion

<p>Barrel: 16.1", 1:13.75" Twist Length: 26.8" - 33.8" Weight: ~6 pounds</p> <p>\$400 (0.025 BTC) amount 0</p>  <p>(more photo)</p>	<p>Barrel: 16.1", 1:13.75" twist Weight(unloaded): 7.5 pounds</p> <p>\$500 (0.0312 BTC) amount 0</p>  <p>(more photo)</p>	<p>Barrel: 16" 4140 steel, 1:9" twist Length: 32" - 35" Weight: 6.5 pounds</p> <p>\$550 (0.0344 BTC) amount 0</p>  <p>(more photo)</p>	
<p>PTR GREEN GI SPECIAL EDITION .308 G3</p> <p>Caliber: .308 Winchester / 7.62x51mm NATO Capacity: One 20 round magazine included Barrel: 18" Match Grade Barrel, 1:10 twist rate Length: 40.5" Weight: 9.5 pounds</p> <p>\$890 (0.0556 BTC) amount 0</p>  <p>(more photo)</p>	<p>CENTURY ZASTAVA N-PAP M70 AK-47</p> <p>Caliber: 7.62x39mm Capacity: Two 30 round magazines included Barrel: 16.25" Hammer Forged Barrel, 1:10" twist Dimensions: 36" long Weight: 7.9 pounds</p> <p>\$590 (0.0369 BTC) amount 0</p>  <p>(more photo)</p>	<p>KRISS VECTOR SDP .45 ACP SPECIAL DUTY PISTOL</p> <p>Caliber: .45 ACP Capacity: One 13 round magazine included Barrel: 5.5", 1:16" twist, threaded muzzle Length: 16" Weight: ~5.4 pounds</p> <p>\$1450 (0.0906 BTC) amount 0</p>  <p>(more photo)</p>	
<p>BLUEGRASS ARMORY MOONSHINER BULLPUP .308 WINCHESTER</p> <p>Caliber: .308 Winchester Capacity: One magazine included Barrel: 21" 4140 Chrome Moly steel tapered heavy barrel, threaded muzzle Dimensions: 36" long Weight: ~12.2 pounds</p> <p>\$2300 (0.1437 BTC) amount 0</p>  <p>(more photo)</p>	<p>CENTURY ARMS CENTURION 39 AK 7.62X39</p> <p>Caliber: 7.62x39MM Capacity: 2 30 Round Tapco magazines included Length: 37.25" Barrel: 16.5", 1:10" Twist</p> <p>\$930 (0.0581 BTC) amount 0</p>  <p>(more photo)</p>	<p>FN SCAR 17S 16.25" 7.62X51</p> <p>Caliber: 7.62x51mm NATO Capacity: One 20 round magazine included Barrel: 16.25" Chrome-Lined Hammer Forged steel Length: 28" with stock folded, 35.5" with stock collapsed, 38" with stock extended Weight (unloaded): ~7.9 pounds</p> <p>\$2450 (0.153 BTC) amount 0</p> 	

<http://5xxqhn7qbtug7cag.onion/>

Case Example

Kidnapping & Sell in Dark Web



<https://www.youtube.com/watch?v=ShUbMBtE8qc>



Pedophilia / Children Kidnapping



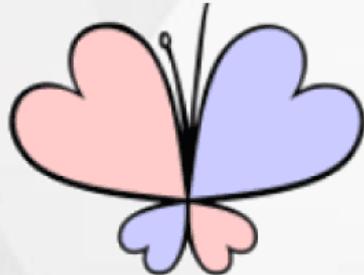
Pedo who's
attracted to boy



Pedo who's
attracted to girl



Pedo who's
attracted to boy



Pedo attracted
no gender

Pedophile Code Words

Found in Podesta E-Mails via WikiLeaks

"hotdog" = boy

"pizza" = girl

"cheese" = little girl

"pasta" = little boy

"ice cream" = male prostitute

"walnut" or nuts = person of colour

"map" = semen

"sauce" = orgy

Case Example

Naked & Smalls

2000+ MOVIES (CP, PEDOMOM, INCEST)

HOMEMADE MOM BLOWJOB FOR BOY

WHEN THE DREAM COMES TRUE FOR CHILD-BOY

LITTLE GIRL SUCKS DICK

Human Torture Video



<https://destrojfqh3impre.onion.ly/>

Human Live Torturing

https://dwkfszqrr6ugdo2t.onion.ly

SPOXXY WELCOMZ YOU TO SICK\$TARTER™! NEXT LIVE EVENT IN 14 DAYZ 15 HOURZ AND 23 MINUTEZ.

Meet Amy from Leedz. Her fate iz in your handz! Decide what happenz, vote with BTC!!



Feeding time at the zoo. Check back laterz!

Option 1: To set Amy free, send to: 1GJYMFsNGfXMq66862AUcfgJZJa56KuNGJ

Option 2: For live torture, rape, and death, send to: 18gtYeKzAlsVTWBPrKSFEevSkTiHz2NRKL

Your vote iz your ticket to the live event. No vote, no entry on the day. Dont forget to save the addrez and come back in 14 dayz 15 hourz and 23 minutez for the live event! Spoxxy luvz red!! Lolz and luvz.

Vote Status:

Free Amy: 0.52 BTC

TRK Amy: 23.41 BTC

<https://dwkfszqrr6ugdo2t.onion.ly/>

Case Example

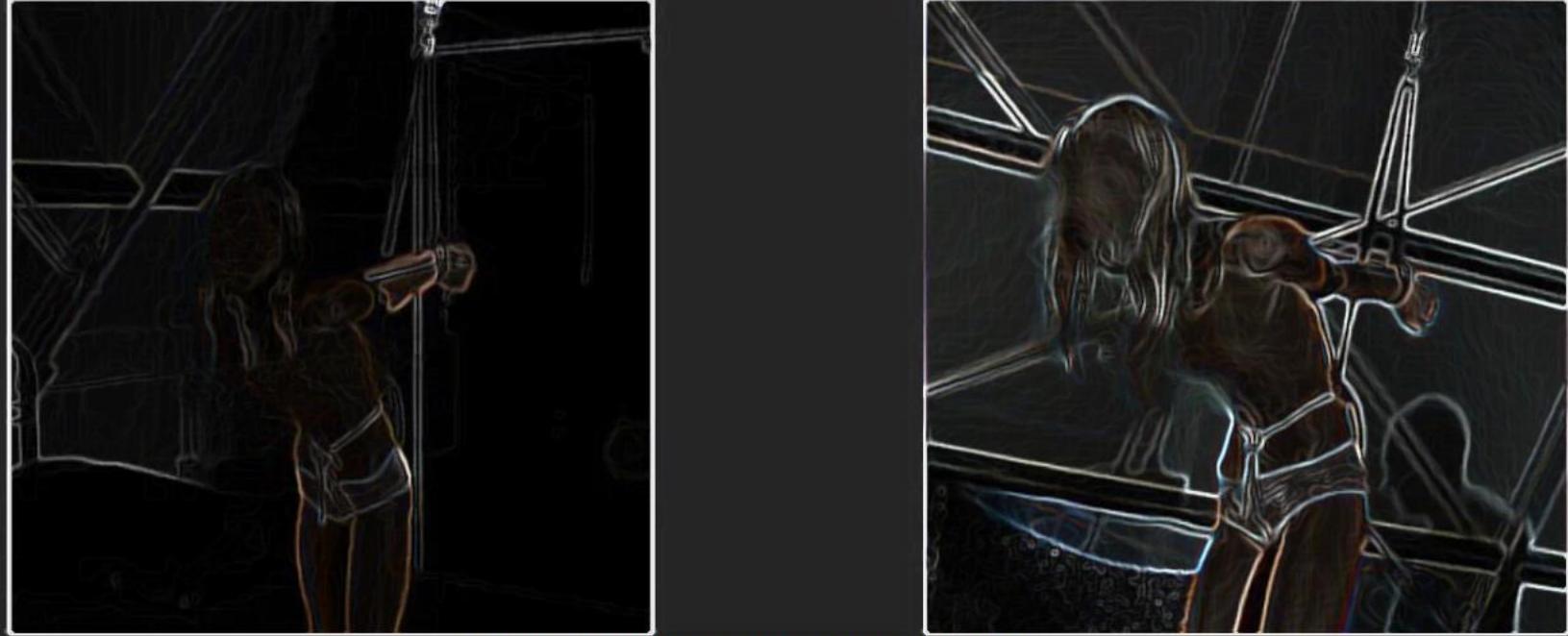
Red Room



<http://redroomifcjbj5qz.onion/>

Human Trafficking

Country of origin: United States
Abducted in: Paris
Held in: EU
Weight: 47kg
Measurements: 32A-24-34
No STD's.



The image consists of two side-by-side photographs of a woman with long dark hair, wearing a dark top and pants. She is bound in a dark, enclosed space, likely a vehicle or a small room, with her hands and feet secured by heavy metal chains attached to the ceiling and floor. Her head is bowed, and she appears distressed. The lighting is dim, and the overall atmosphere is one of confinement and abuse.



Please Join OSINT Indonesia Community

https://t.me/OSINT_ID

Contact me : @camorra_13