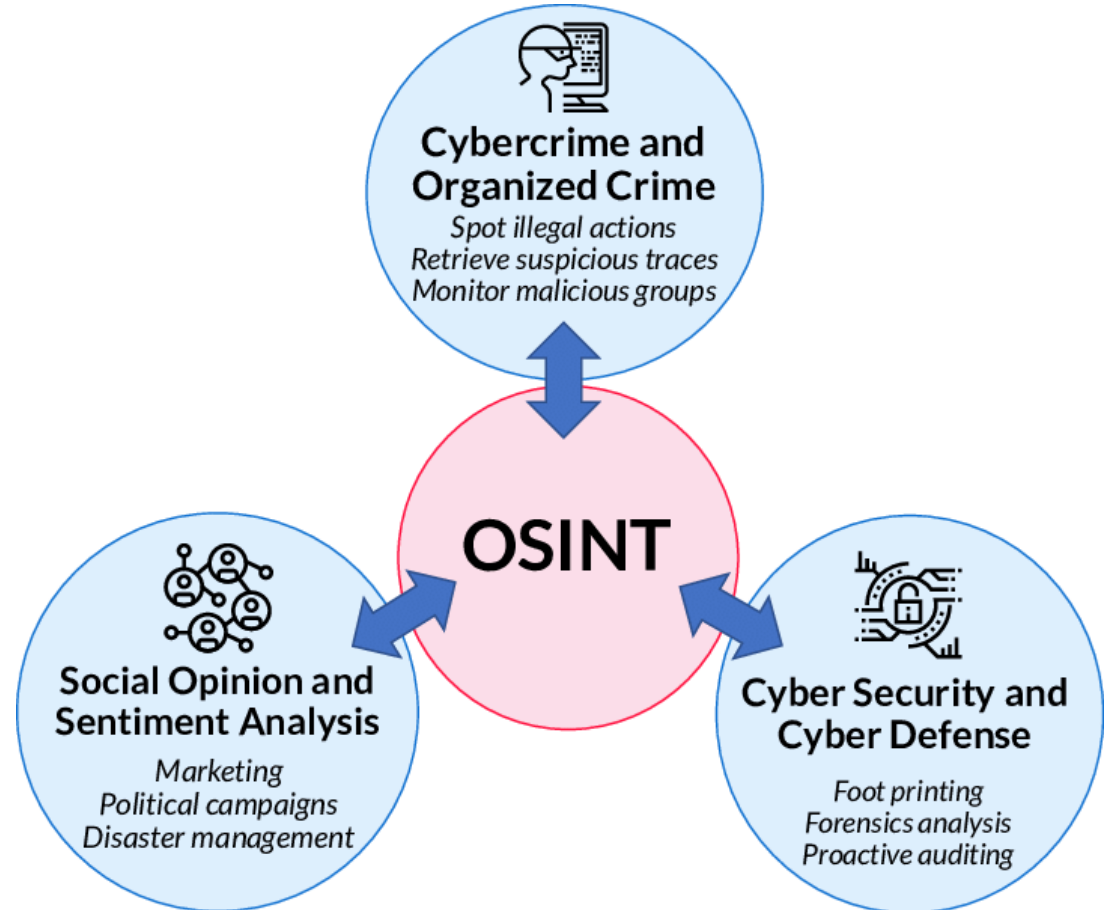


Weaponize the Dark Web for OSINT

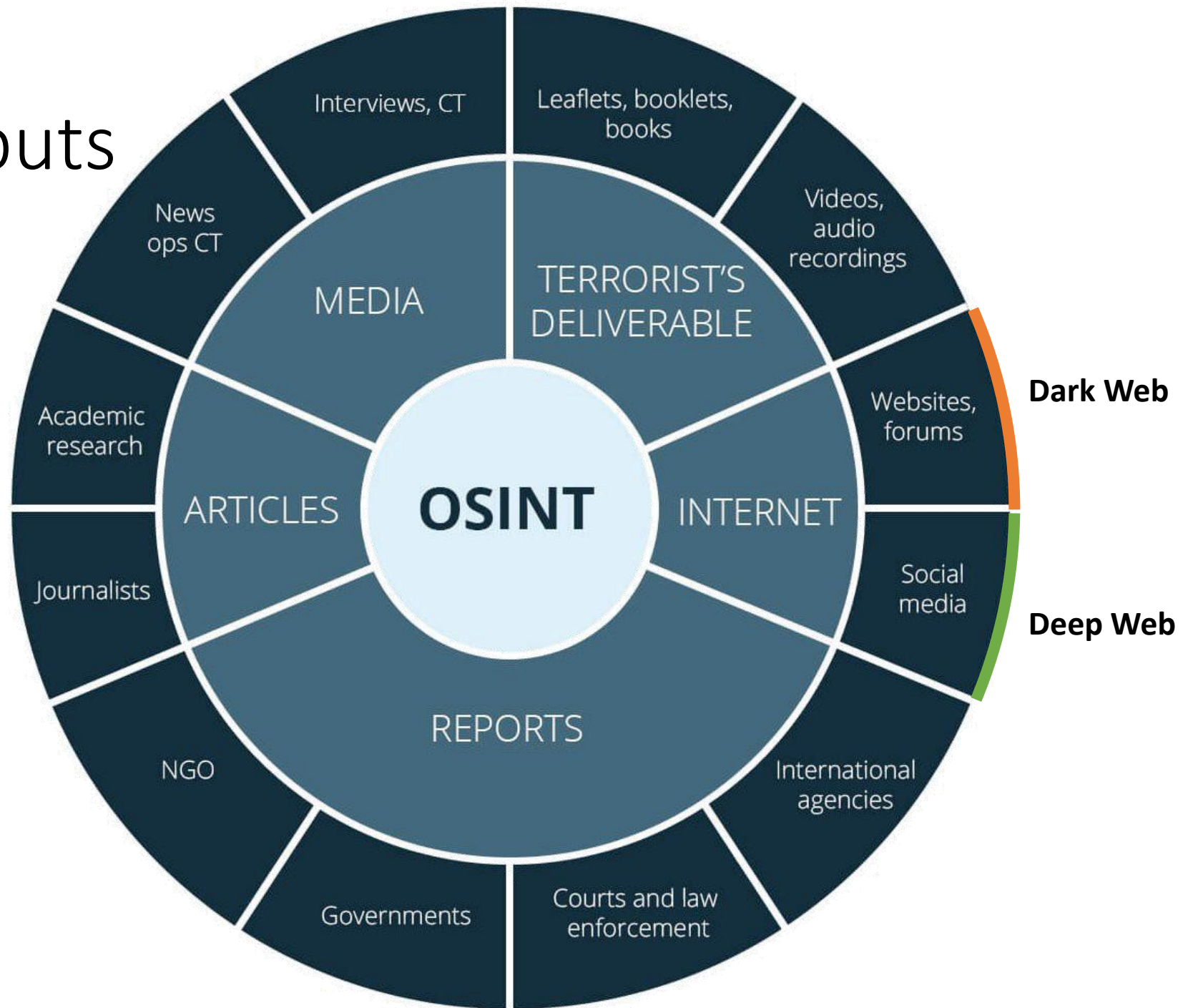
Georgios Pouraimis, PhD

Open-Source Intelligence (OSINT)

Open-Source Intelligence (OSINT) is the intelligence collected from the sources which are present openly in the public



OSINT Inputs

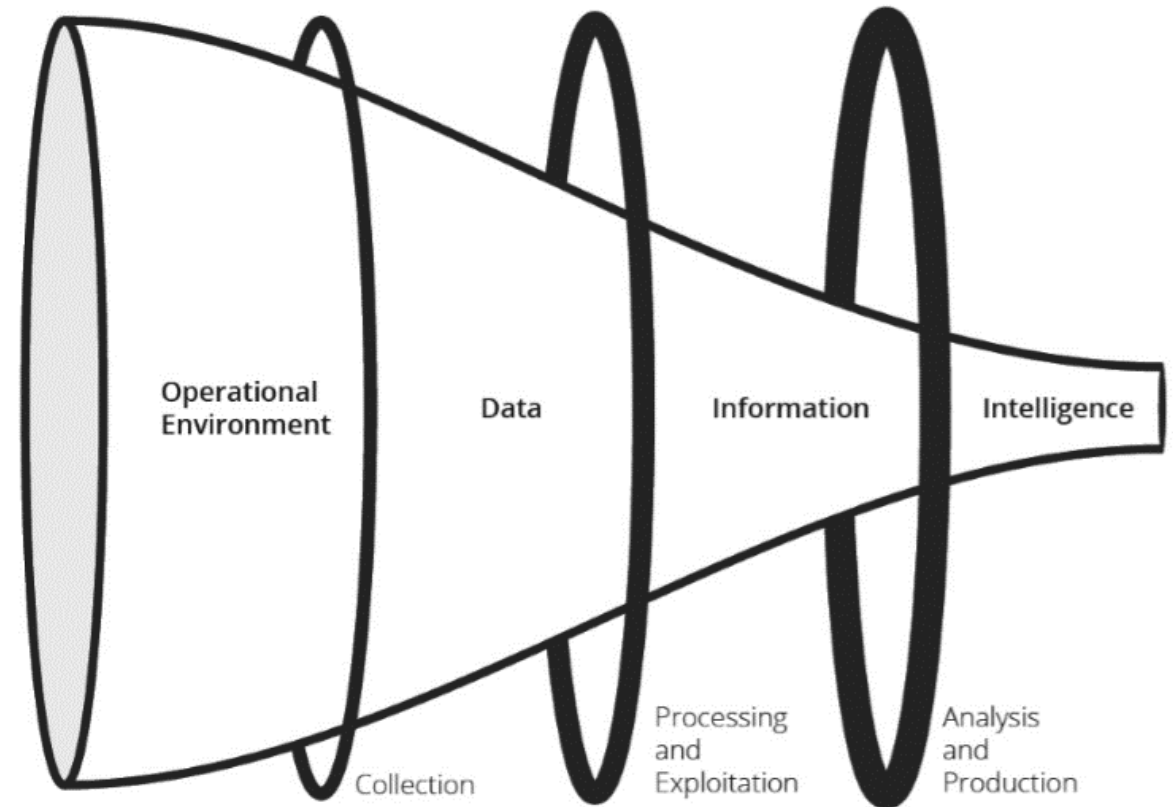


Data, Information, Intelligence

Data: the collection of snapshots of an event

Information: data from an event and put it into a narrative

Intelligence: uses information to drive decisions



OSINT Inputs

- Structured data sources



- IP whitelists/ blacklists - CVEs
- Feed/web scraper – Parser

- Unstructured data sources



- News sites - Twitter
- Feed/web scraper - Natural Language
- Machine learning techniques - NLP tools

- Dark web

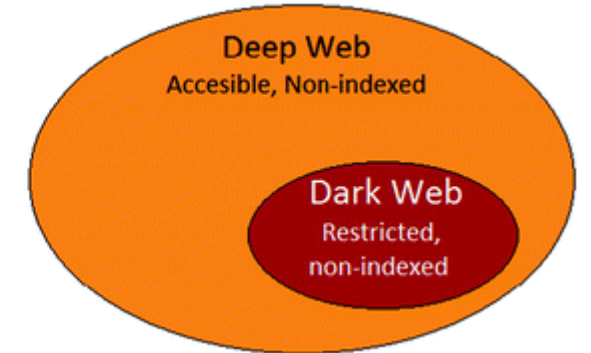


- Forums – Marketplaces
- Dark web access - Dark web scraper - NLP tools
- Machine learning techniques

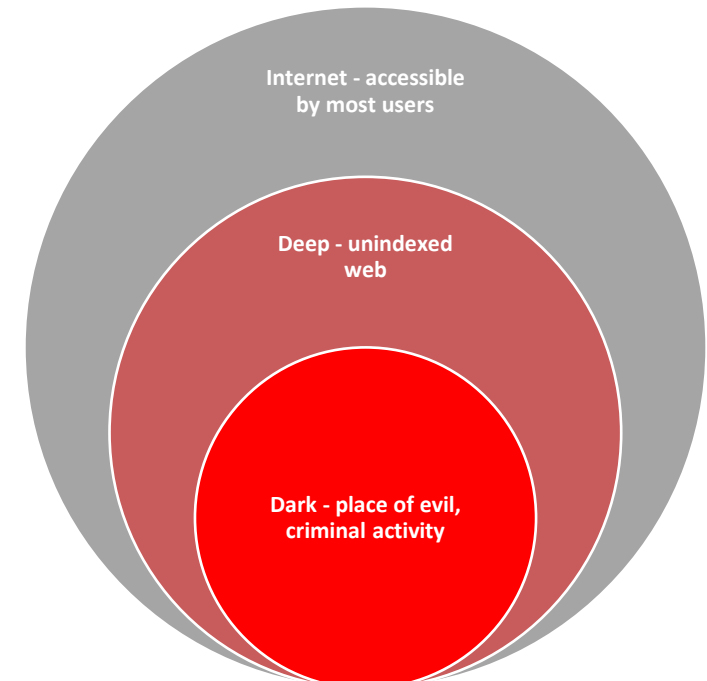
Levels of the Internet: Simple Version

- Daniel Miessler has a blog post' that shows the relationships more simply
- Dark Web is inside the Deep Web
- Deep Web is inside the Internet
- It is all about accessibility: who can access what data from where

World Wide Web



OR



Surface, Deep, and Dark Definitions

- Three distinct layers of the Internet:
 - Surface - Easy to access
 - Deep - More challenging
 - Dark - Special techniques
- Most images showing the distinction between them show levels of an ocean



Searching on the Internet today can be compared to dragging a net across the surface of the ocean. While a great deal may be caught in the net, there is still a wealth information that is deep, and therefore, missed.

Michael Bergman's 2001 "The Deep Web: Surfacing Hidden Value"

Deep Web Who and What

- Who uses it:
 - Anyone
 - Everyone
 - Must know about or be able to find the resources without search engines
- Gray area between Surface and Deep with sites moving between them
- Example Services:
 - Business networks
 - Unlinked web sites (using IP addresses instead of domain names)
 - Banks, investments, financial
 - Government information about you
 - Social media (private)
 - File-sharing sites

Dark Web Who and What

- Who uses it:

- Journalists
- Oppressed people
- Criminals
- Governments/Law Enforcement
- Privacy-minded people
- Whistle-blowers

- Example Services:

- Anonymous browsing
- Anonymous communications
- Anonymous file-sharing
- Unlinked web sites
- Forums about any topic
- Criminal marketplaces
- Specialized Dark Web search engines

OSINT in the Dark Web

- Why OSINT analysts need the Dark Web?
 - Curiosity
 - Protect your communications
 - Use it to anonymize your traffic/activities
 - Follow target activities
 - Track financial fraud
 - Support Law Enforcement and Intelligence Agencies

Using Search Engines to Find Deep Web

Google

deep web sources

Ολα Εικόνες Ειδήσεις Βίντεο Χάρτες Περισσότερα Ρυθμίσεις Εργαλεία

Περίπου 922.000.000 αποτελέσματα (0,59 δευτερόλεπτα)

Deep Web search engines

- BizNar.
- DATA.GOV.
- Google News.
- Google Scholar.
- govinfo.
- GreyNet International.
- **Internet** Archive (including Wayback Machine)
- OpenGrey.

Microsoft Bing

deep web sources

ALL WORK IMAGES VIDEOS NEWS

40,000,000 Results

Analysts can search the "invisible web", or **deep web sources**, including public records and social networks. By combining and re-combining information from these searches, they can uncover information and connections that are otherwise difficult to find.

[Conducting Online Investigations Using Deep Web Resources](#)
i-sight.com/resources/conducting-online-investigations-using-deep-web-resourc...

Was this helpful? 👍 🗨

🟢 [Top 10 best websites to explore in the Deep Web - Blog ...](#)
<https://www.masterdc.com/blog/best-websites-in-the-deep-web>
11/6/2018 - To access the Deep Web it is necessary that you use special search engines. The safest and the best developed so far is Tor (The Onion Router). Learn more: what are the differences between the...
4/5 ★★★★★ (15) Estimated Reading Time: 6 mins

Yandex

deep web sources

Web Images Video News Translate Disk Mail Ads

🔗 [Deep web links | Deep web sites | The Deepweb 2021](#) 8 million results found
[deepwebsiteslinks.com](#)
The deep web links 2021 - looking working dark web sites link, The hidden wiki, .onion ... onion links, deep web link 2021 and tor directory etc. If you do, then you've landed on the...
[Porn](#) · [121+ Active Deep Web Links](#) · [Anonymous Emails Links](#)

🔗 [Deep Web Sites 2021 | Dark Web | Deep Web Links](#)
[deepweb-sites.com](#)
The Deep Web Sites, Dark web, Hidden Wiki is accessed using Tor that contains .onion websites and provided Deep Web Links 2021 with more of deep web news.
[Deep Web Links](#) · [Best VPN](#) · [Tor](#) · [News](#)

WARNING!

The Dark Web contains illegal, unethical, and disturbing content! BEFORE using it ensure you and your organization know the risks .



Dark Web Risks

- Consider your work location before accessing the Dark Web

Who else can view your screen?

Is the sound on your computer on?

What security precautions are on your computer operating system and in your browser?

- Some risks to consider include:
Viewing child pornography

Malicious files

Revealing information about you or your organization

Attacks against your browser and computer system

Is Your Organization OK with Dark Web Use?

- One more slide on REALLY making sure that your organization and your customer are REALLY OK with you taking your work into the Dark Web
- Some managers will say it is fine and you should check with your legal department and/or senior management
- Get approvals for this work in writing before doing it

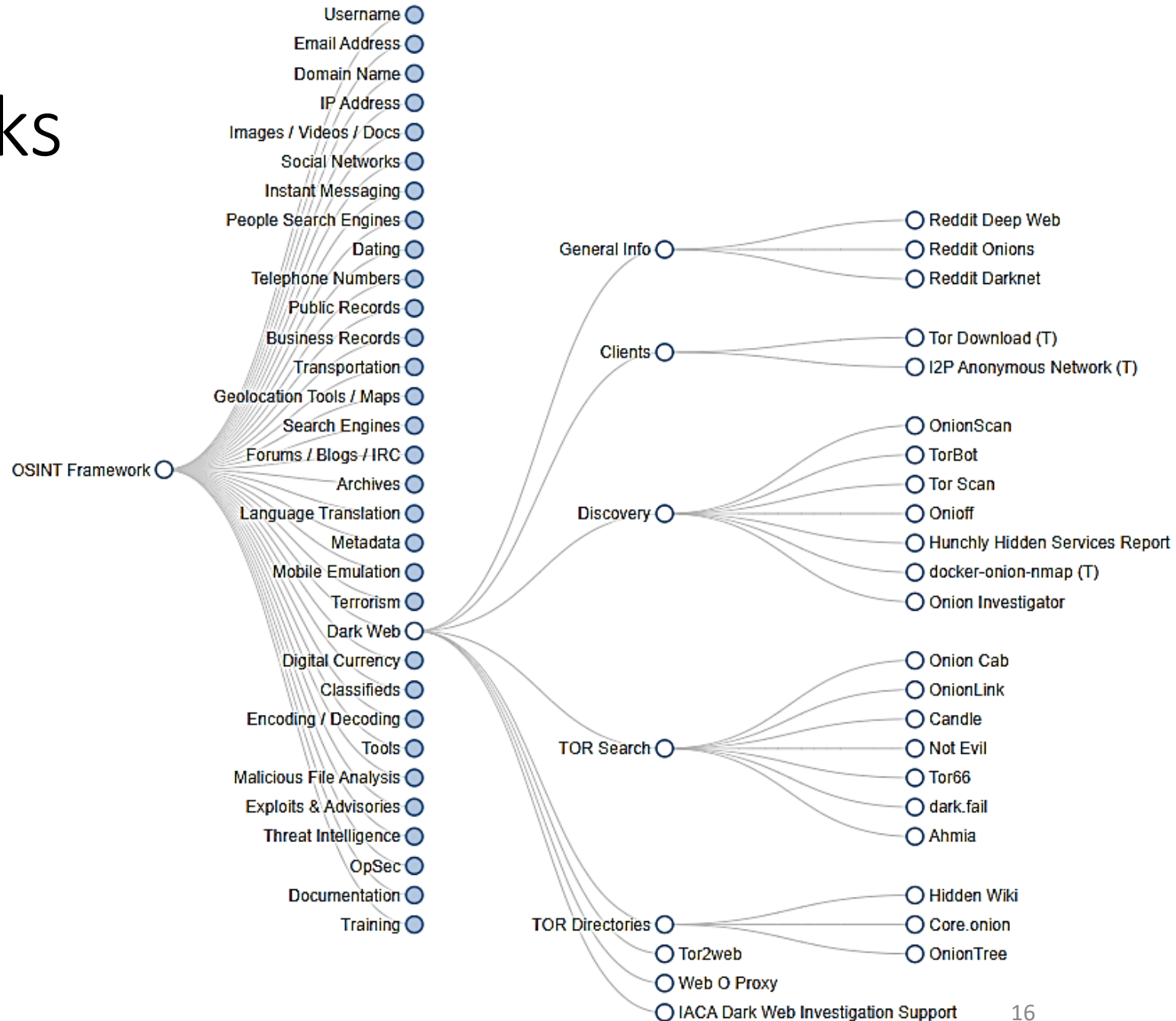
Welcome to the Dark Web!



- The Dark Web consists of "overlay networks" that use special software
- Let's talk about the 3 most common Dark Web networks:
 - Freenet
 - I2P
 - Tor

OSINT Frameworks

- Collection of OSINT tools
- Used by security researchers and penetration testers



OSINT Tools

Free tools

sherlock-project/sherlock
twintproject/twint
mxrch/Ghunt
qeeqbox/social-analyzer
s0md3v/Photon
smicallef/spiderfoot
Jofpin/trape
laramies/theHarvester
sundowndev/phoneinfoga
instaloader/instaloader
...and many more

Commercial tools

Maltego (with bundles)
Pipl
NesusXlore (with features)
SpiderFoot
ChipherTrace
Domain Tools
RocketReach
Hunchly
Sn1per
...and many more

OSINT Web Based Tools

The screenshot shows a web browser at the URL start.me/p/wMdQMQ/tools. The browser's address bar and navigation icons are visible at the top. Below the address bar, there is a navigation menu with tabs for "Technisette", "Addons", "Databases", "OSINT", "Search engines", "Tools", and "Tutorials". The "Tools" tab is currently selected.

The main content area is divided into two columns. The left column features a section titled "TOOLS - DARKWEB" with the subtitle "Tools for investigating darkweb". It lists the following tools:

- Deepdotweb - List of most popular darkmarkets
- DeepWeb - Deeplinks
- DeepWeb - Top 50 onion-sites
- Hunchly's Darkweb report
- i2p (download)
- Ichidan (visit via Tor)
- Onionscan
- OnionShare
- Tor (download)
- TorNodes
- Zeronet (download)

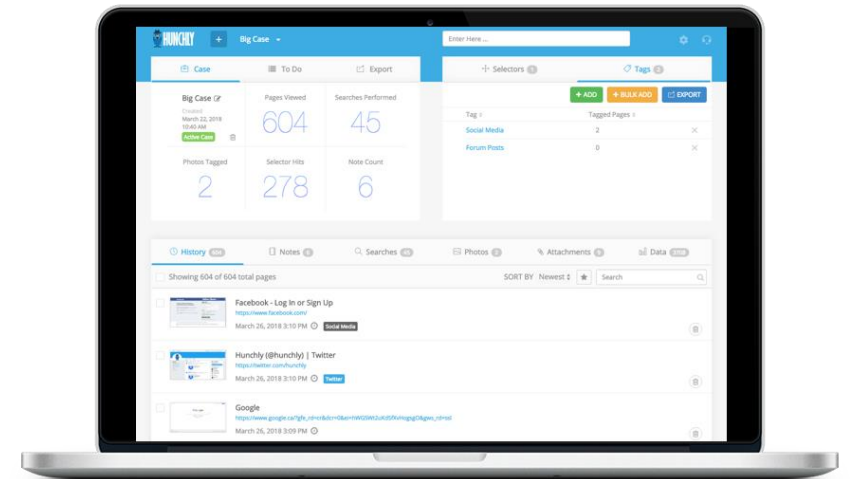
The right column features a section titled "TOOLS - OSINT" with the subtitle "Tools, flowcharts and cheatsheets to help you do your OSINT research". It lists the following tools:

- 101+ OSINT resources
- AnswerThePublic
- Bellingcat - OSINT Links
- Browsershots
- Browsershots (screenshot via mobile device)
- Cheatsheet Bing search (NL)
- Cheatsheet Duckduckgo search (NL)
- Cheatsheet Yandex search(NL)
- CloudFail - find IPs behind Cloudflare
- Cyberchef
- Databasic
- Datawrapper
- DFIR Training - Various tools
- Digital Methods Initiative Tool database

<https://start.me/p/wMdQMQ/tools>

Hunchly Daily Hidden Services Report

- Justin Seitz runs crawler software in the Tor network and discovers new hidden services
- The XLSX can be emailed to you if you sign up or you can download from the Hunchly Twitter feed
- <https://darkweb.hunch.ly/>
- <https://twitter.com/hunchly>



Download today at www.hunch.ly

Hunchly

Hunchly 2.3.1

test case

Search

Case	To Do	Export
test case Created March 8, 2022 2:31 PM Active Case	Pages viewed 7	Searches 0
Captioned images 0	Selector matches 5	Notes taken 0

Selectors 1	Tags 0
+ Adding a new selector will scan all case files for the new selector. This may take a minute or two.	
+ Add + Bulk add Export matches	
Selector	Count
Ukraine War	5

History 7	Notes 0	Images 0	Attachments 6	Searches 0	Data 97
History of all pages you have viewed for this case are listed here from newest to oldest.					
Showing 7 of 7 total pages					
Sort by Newest					
Search titles and URLs					
<input type="checkbox"/>	Preview unavailable	Listen to Offradio Live - Coeus - Vita https://www.offradio.gr/		March 9, 2022 2:53 PM	



Dashboard

Capture

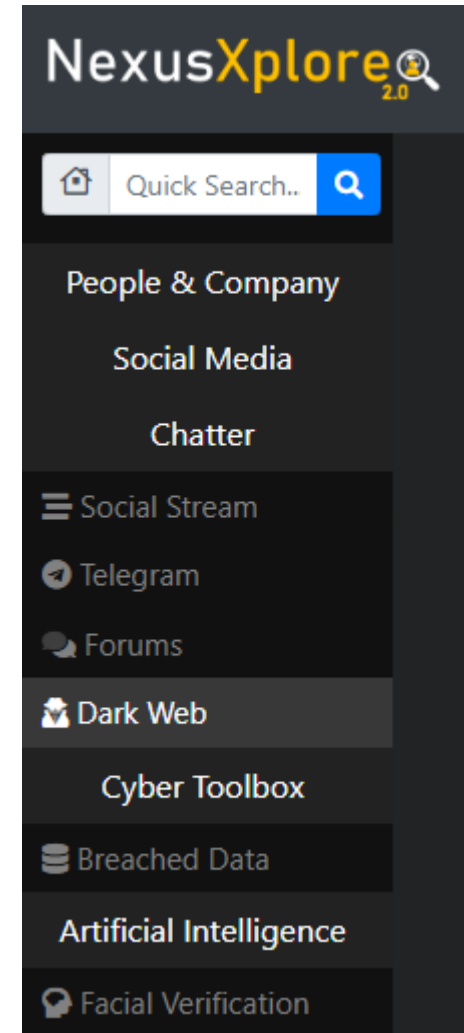
Case test case

Queue 0 Selectors 0 Notes 0 Tags 0

NexusXplore

- NexusXplore is a software used in enabling advanced search & enhancing efficiencies in the collection & analysis of publicly available information through a single interface.
- An investigator can Find & explore people, places & information across social media, surface, deep & dark web, observe geographical areas for situational awareness, find documents & use artificial intelligence for image analysis & translation to support your operations
- It is Used & trusted by federal law enforcement, national security agencies, global banks & Fortune 500s around the world. A product built from experience

https://nexusxplore.app/gc_current.php
<https://www.nexusxplore.com/>



NexusXplore

NexusXplore 2.0 Visual Graph Geo Lens What's New Case Files Images AI

Quick Search.. Dark Web Clear Page Results Keyword Highlight: Settings Home Telegram Forums Dark Web Cyber Toolbox Breached Data Artificial Intelligence Facial Verification

People & Company Search & Explore Network Activity

Social Media

Chatter

Social Stream

Telegram

Forums

Dark Web

Cyber Toolbox

Breached Data

Artificial Intelligence

Facial Verification

Search Dark & Deep Web:

Query Builder Date Range:

File Type or Extension: PDF Word Excel PowerPoint Archive File

Results language filter...

Sort by Date Sort by Relevance

Data Sources Crypto Filters Passport Filters

Explore Markets, Vendors & Forums

Find vendor, forum, market... Found Markets

Vendors Markets Forums

Launch TOR Safe Research Portal

Dark Web News

Results (1238)

Copy Excel CSV PDF Search:

Domain	Snippet	Date Crawled	View
telegram.me	... pros availableus PICKUPS AND SHIPPING AVAILABLE FOR EYE'S ORDERSus AVAILABLE PHYSICAL IDS PASSPORT CARD SSN CARD 2022-07-05T23:52:17Z Seconds (debit card tipped) TAP TAP** 2022-07-05T23:49:02 user_955496566 kingss1100 kinG wrote: https://t.me/freeknowledgensauce 2022-07-05T23:49:29 user_53875868...		Expand
uni3mtemb5apqu3u2fggdh4ubn7k645wxe53nt62jlvwnicyb4pxid.onion	...y food prices are going, might be a good way to get punters through the door load more comments (1) 26326312 44 points 1 month ago 26326312 44 points 1 month ago Don't see enough of them these days. Nothing better than rocking up to a countryside pub on a Sunday and going home with...	2022-07-05T23:09:11Z	Expand
1BLogC9LN4oPDcruNz3qo1ysa133E9AGg8	...wsfeedFollowing Demo for decentralized, self publishing blogging platform. Create new blog How does ZeroNet work? Site development tutorial ZeroNet documents Source code Enhanced ZeroBlog by zeronetscript Latest comments: williammolina: Nice @ How to have a blog like this te...	2022-07-05T23:04:44Z	Expand
2a2a2abbjsjcwfozjp6idfxsyowoi3ajqyehqzfqyexzhacur7oyd.onion	...ard Cloned Carding Hacking Drugs Dumps Paypal Hack Free Bitcoin Money Counterfeit Cash Buy Gun Gift Passport Visa Mastercard Amex Verified Trusted Bitcoins Escrow Top Hidden Wiki Onion Links Forum Shop FAQ Escrow Shipping Payment Vendor News 0 Total \$0.00 0 items	2022-07-05T22:29:56Z	Expand

Copyright © NexusXplore | EULA | Training | User Guide

Sum-up

- Dark and Deep Web part of our OSINT inputs
- Dark web mostly contains unstructured data sources
- Dark web provides data for terrorists, drugs, weapons, leaks etc
- Need to know our risks!
- Use of frameworks and tools

Thank you!

Questions