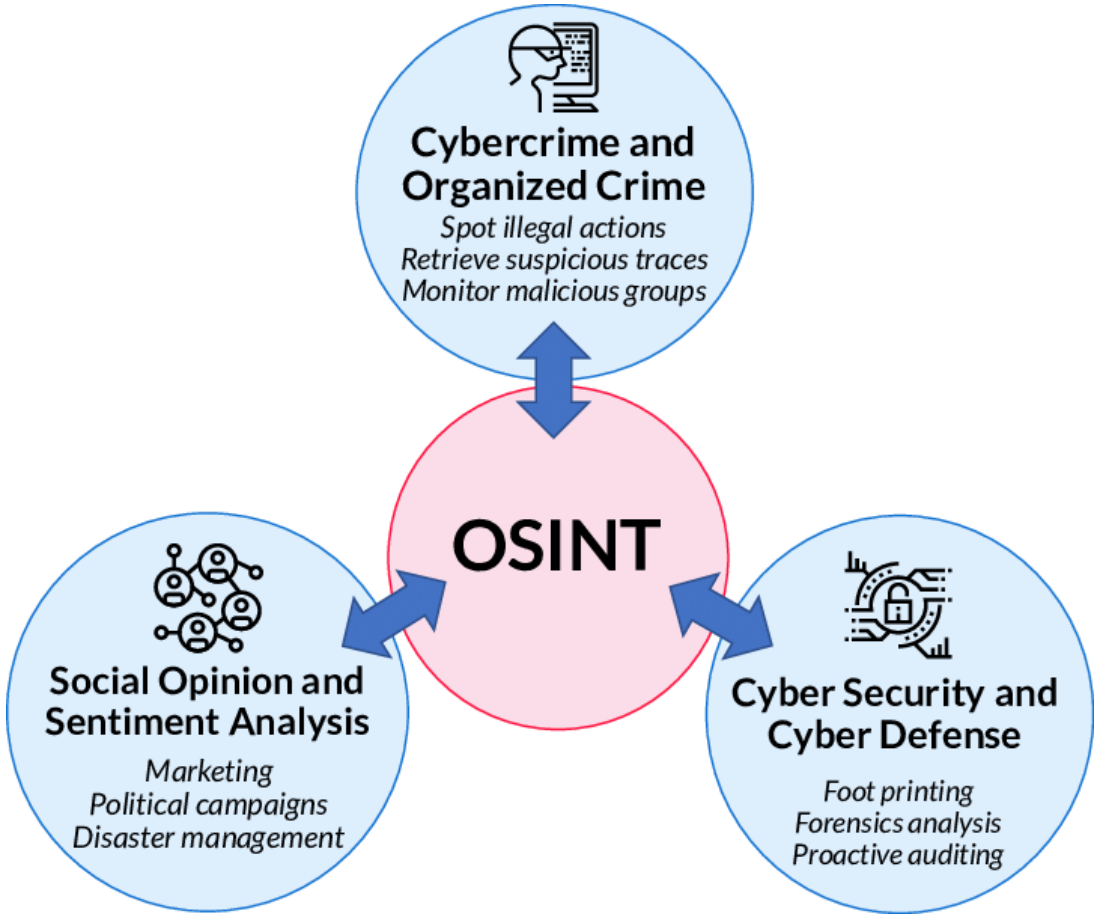
Weaponize the Dark Web for OSINT

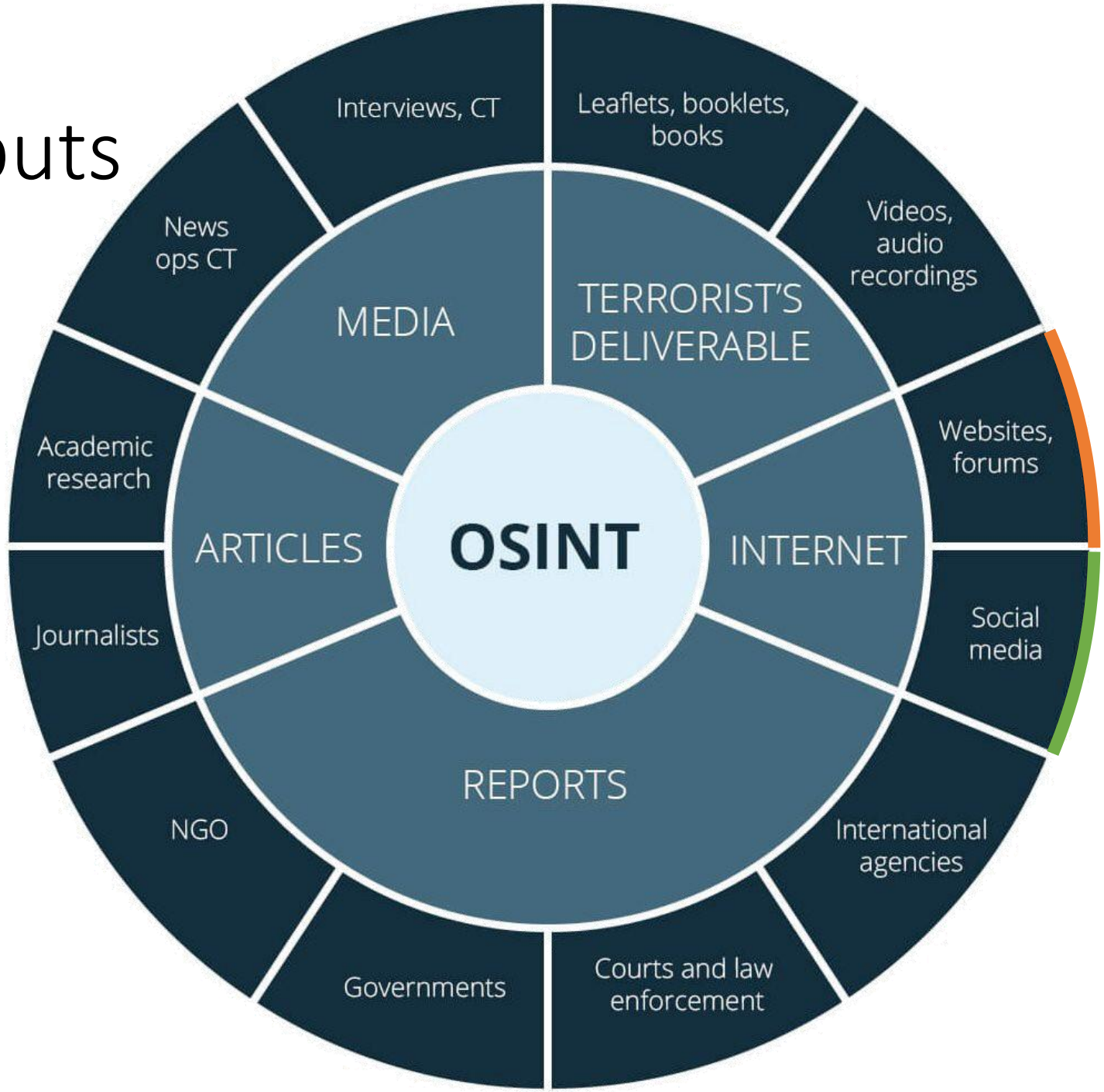
Georgios Pouraimis, PhD

Open-Source Intelligence (OSINT)

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



OSINT Inputs

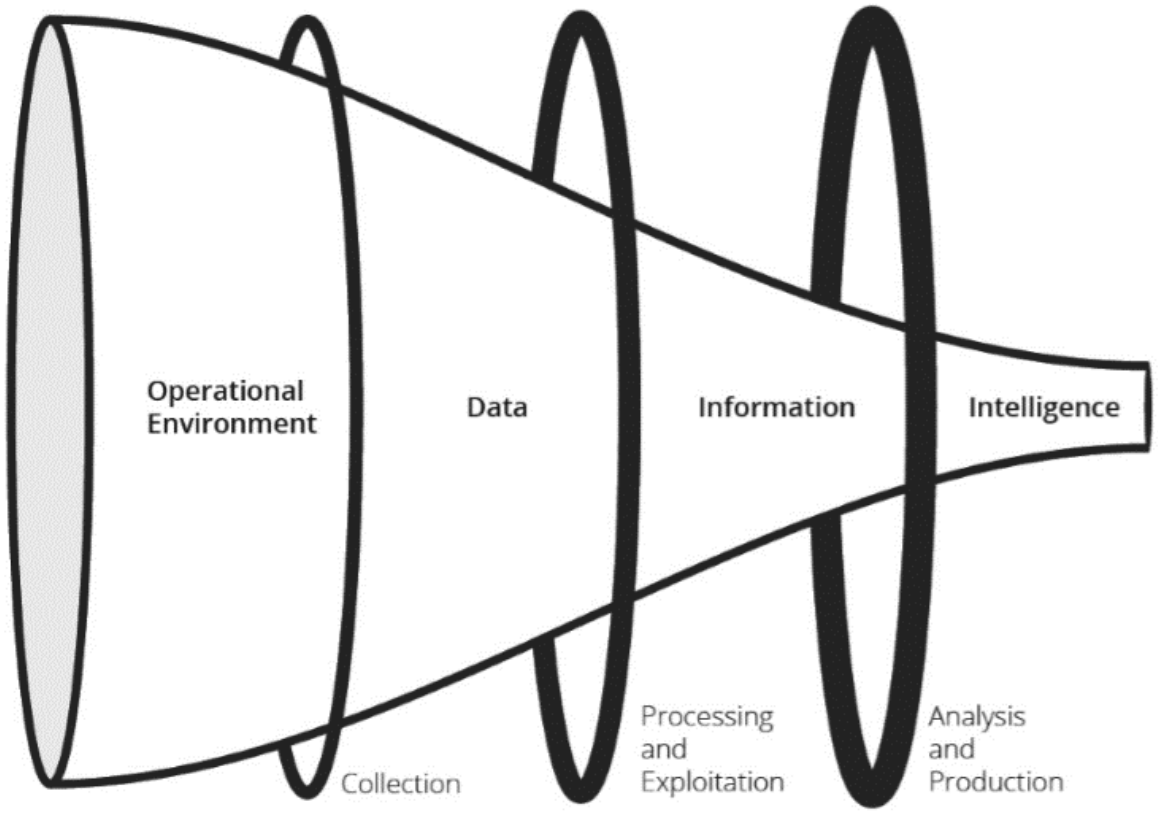


Data, Information, Intelligence

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

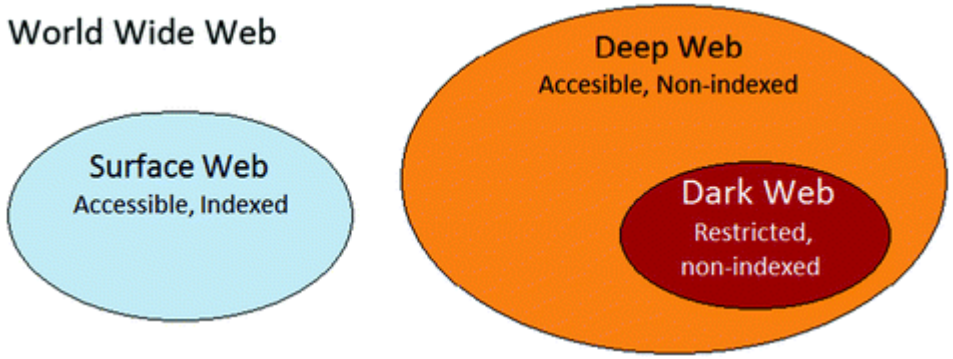
- Structured data sources
  - IP whitelists/ blacklists - CVEs
  - Feed/web scraper – Parser
- Unstructured data sources
  - News sites - Twitter
  - Feed/web scraper - Natural Language
  - Machine learning techniques - NLP tools
- Dark web
  - Forums – Marketplaces
  - Dark web access - Dark web scraper - NLP tools
  - Machine learning techniques

Levels of the Internet: Simple Version

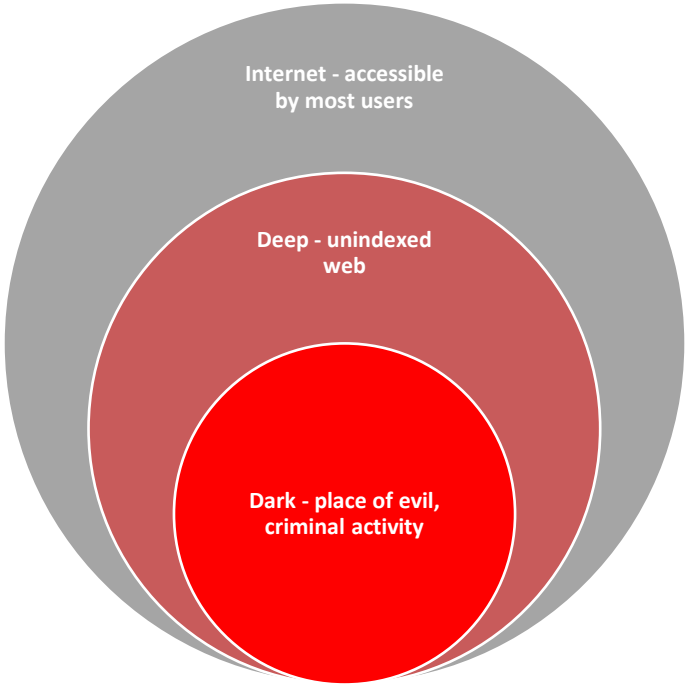
- Daniel Miessler has a blog post' that shows the relationships more simply

- 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

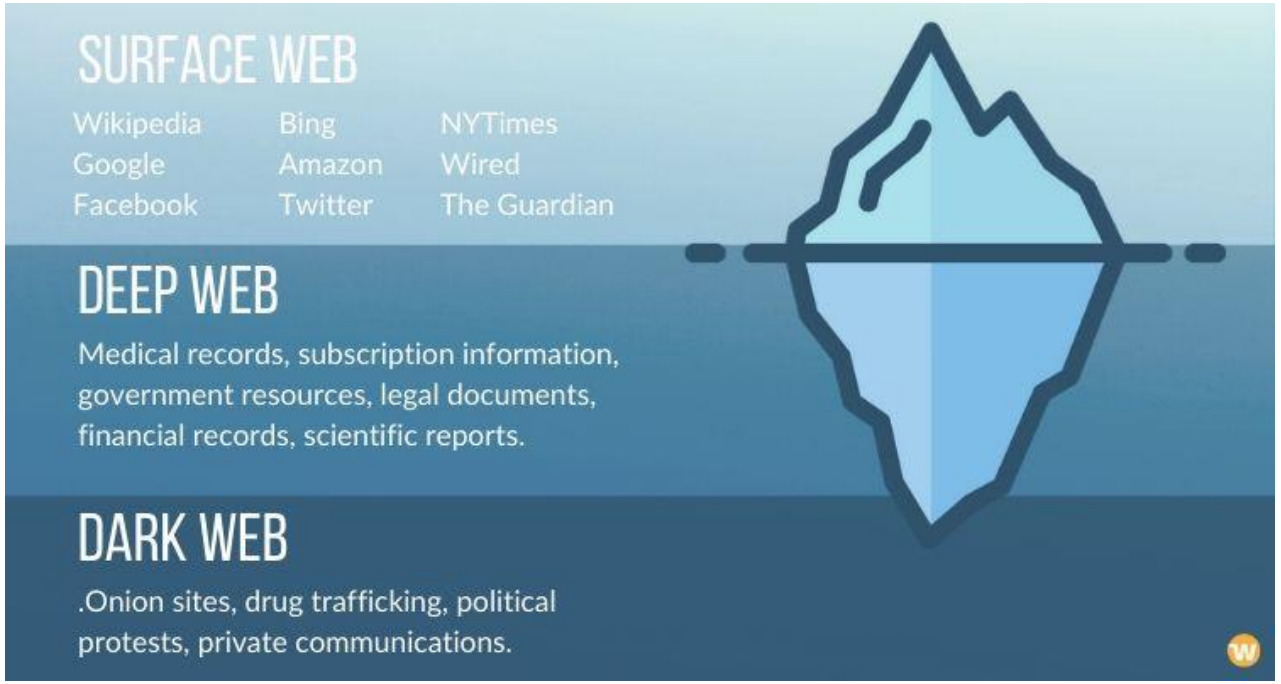


OR



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

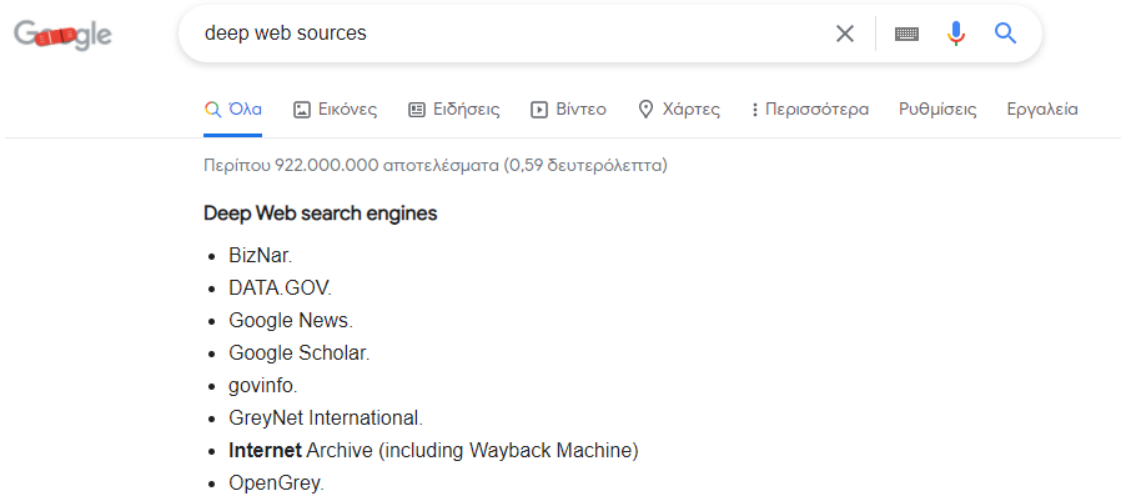
Dark Web Who and What

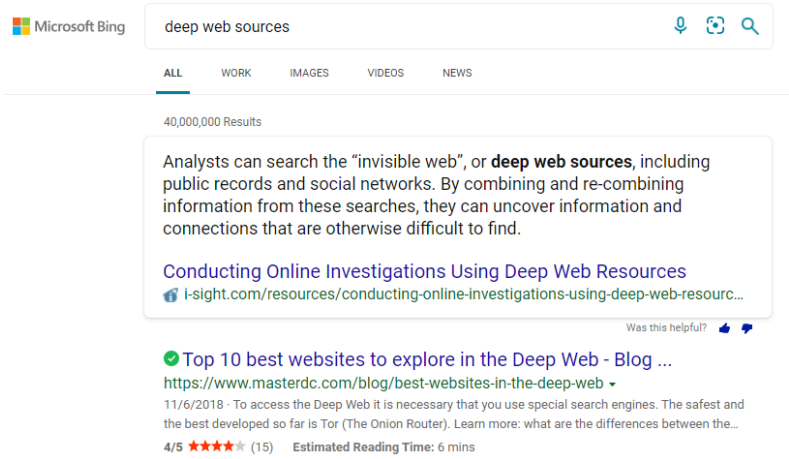
- Who uses it:
  - Journalists
  - Oppressed people
  - Criminals
  - Governments/Law Enforcement
  - Privacy-minded people
  - Whistle-blowers
- Example Services:
  - Anonymous browsing
  - Anonymous communications
  - Anonymous file-sharing
  - Unlinked web sites
  - Forums about any topic
  - Criminal marketplaces
  - Specialized Dark Web search engines

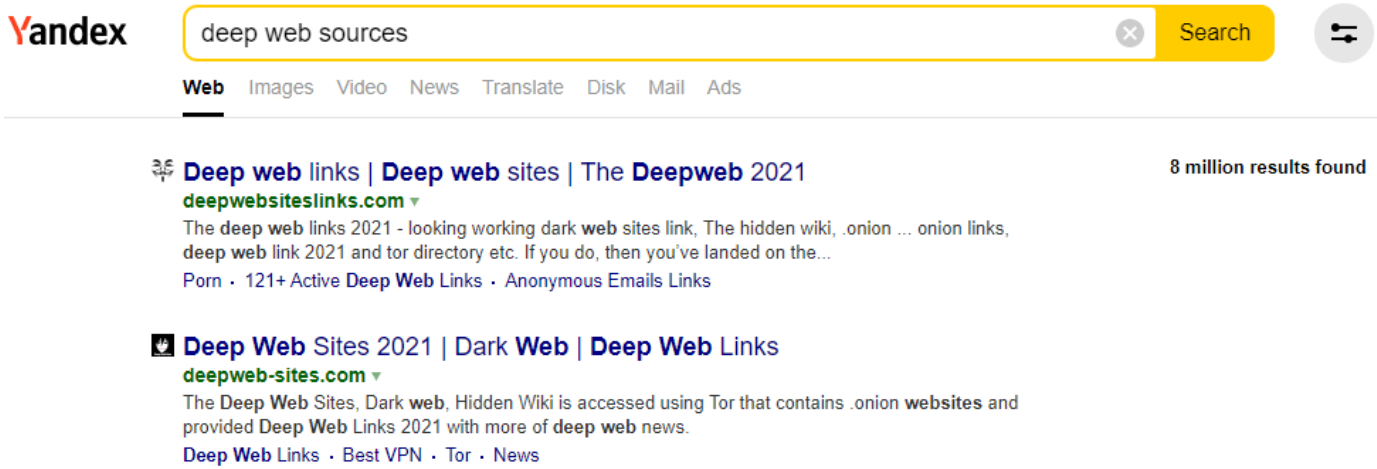
OSINT in the Dark Web

- 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







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

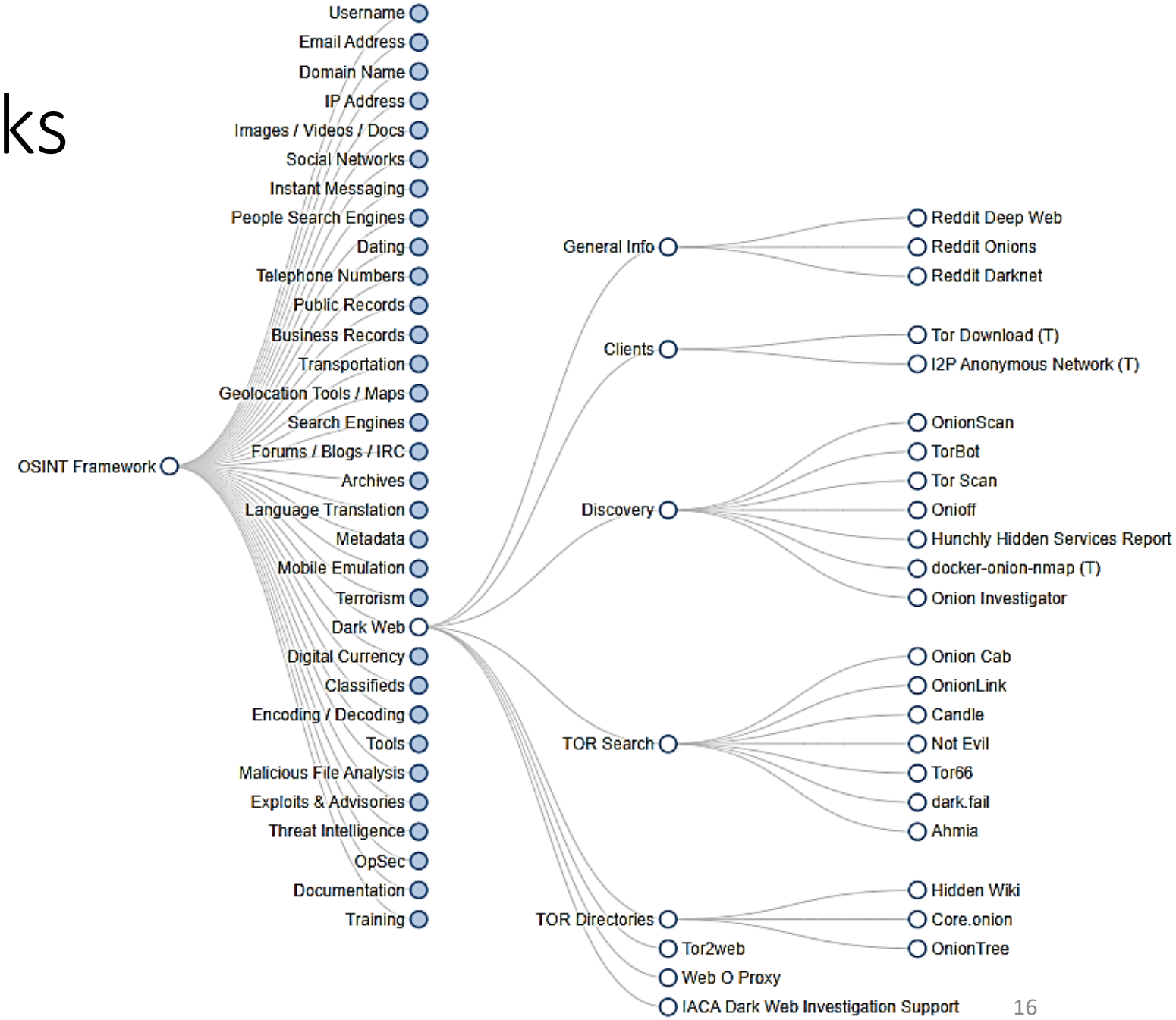
- Get approvals for this work in writing before doing it

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



https://osintframework.com/

OSINT Tools

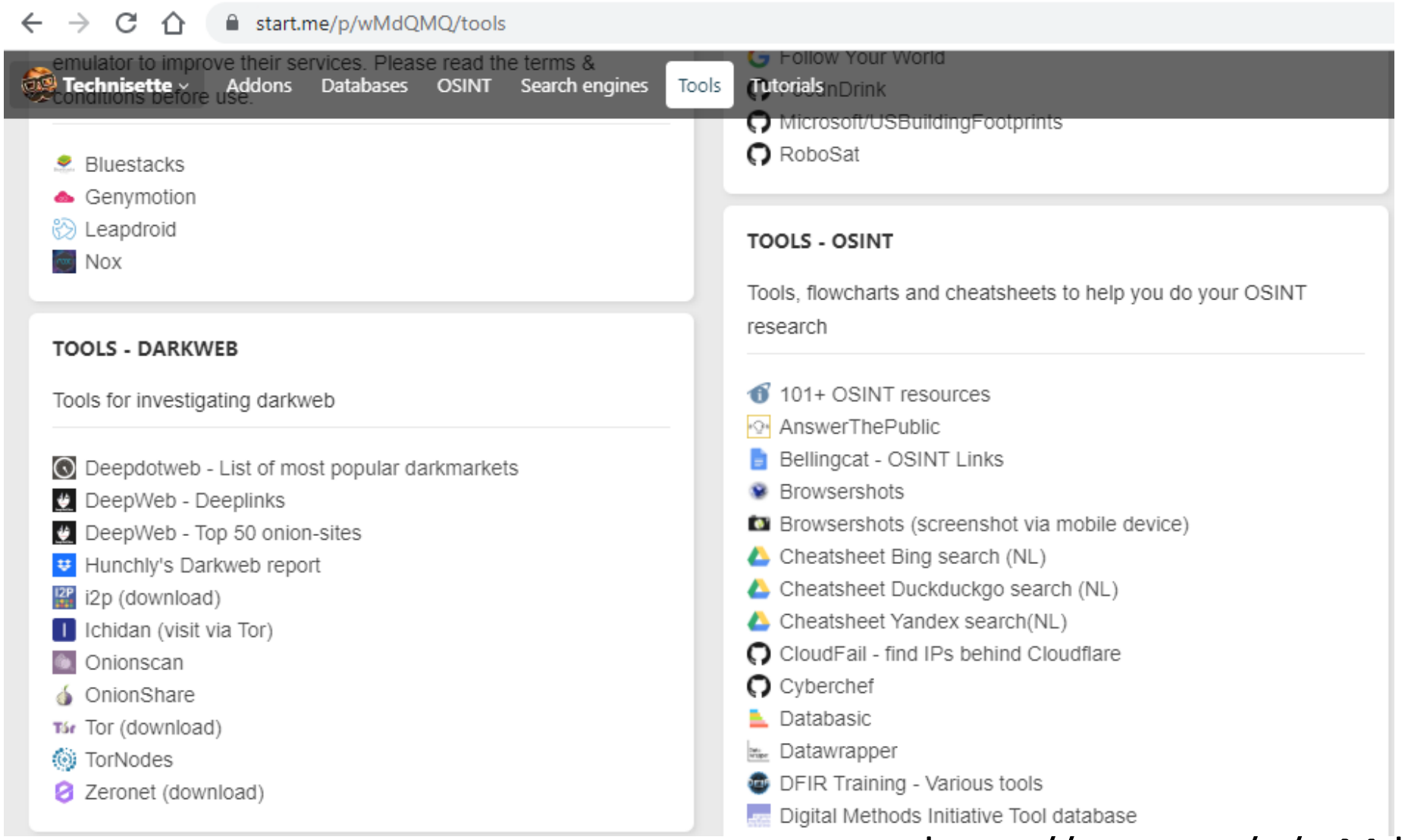
Free tools

- 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



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

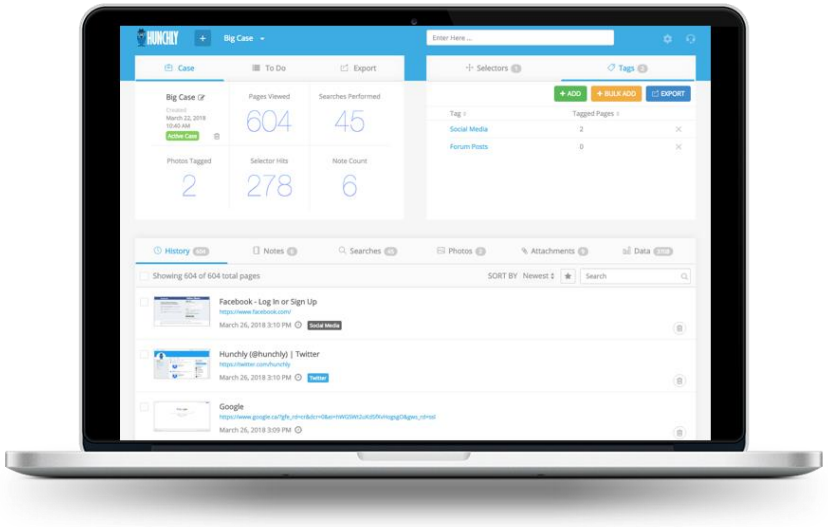
Hunchly Daily Hidden Services Report

- Justin Seitz runs crawler software in the Tor network and discovers new hidden services

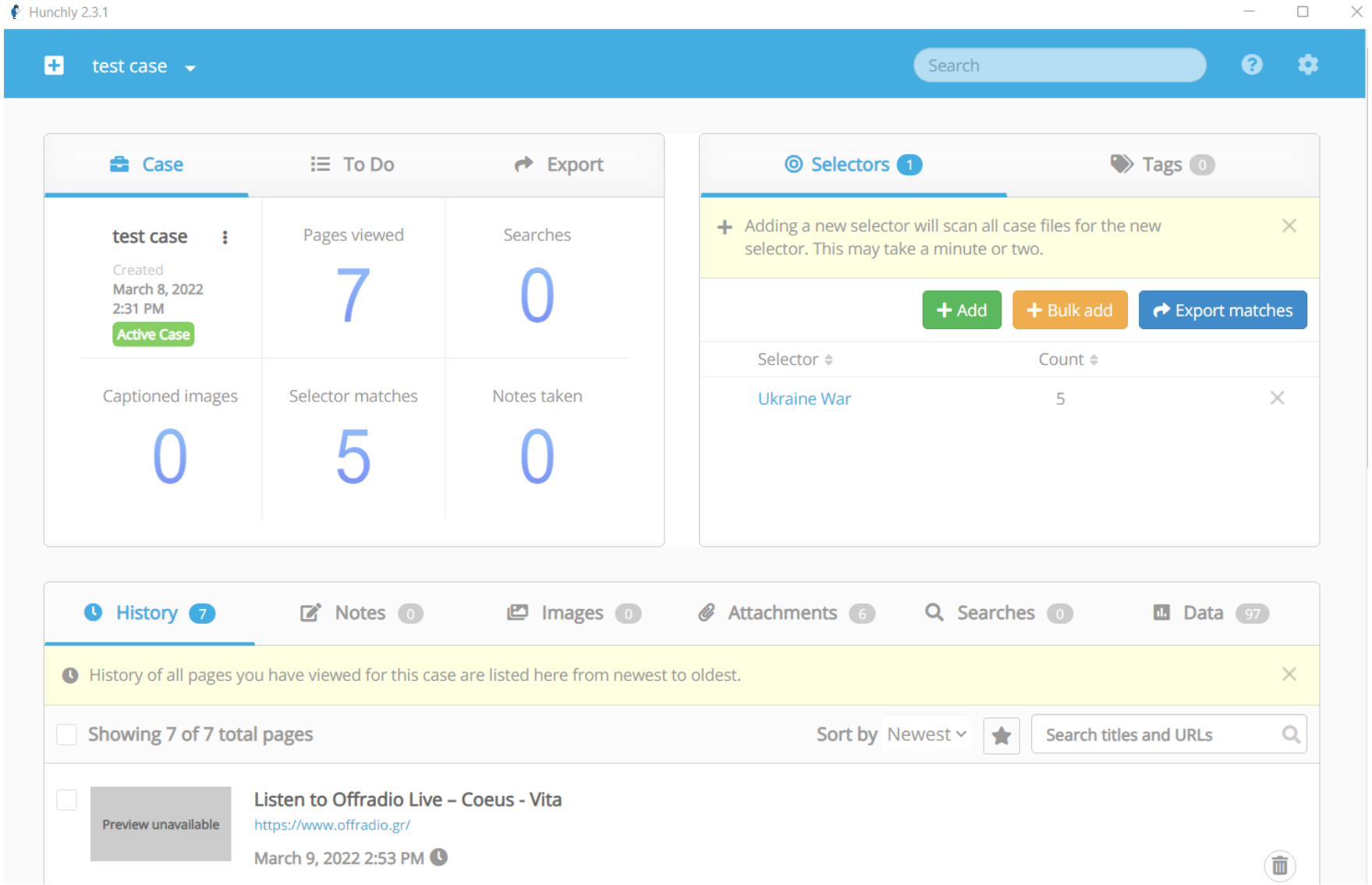
- The XLSX can be emailed to you if you sign up or you can download from the Hunchly Twitter feed

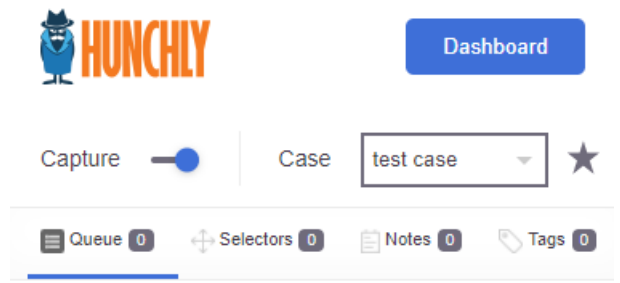
•https://darkweb.hunch.ly/

•https://twitter.com/hunchly



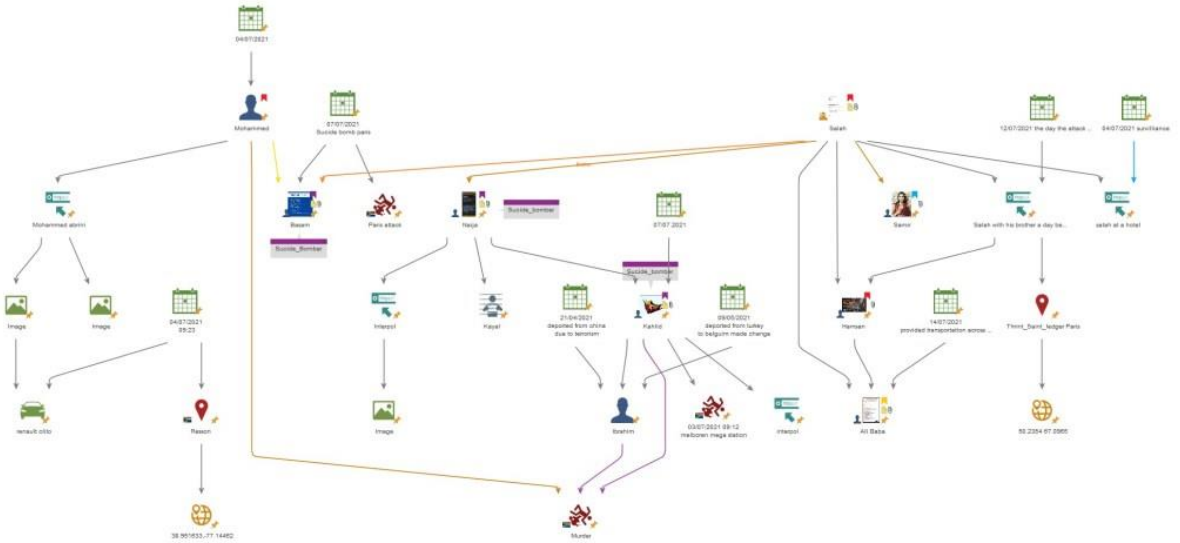
Hunchly


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
Preview unavailable
Listen to Offradio Live – Coeus - Vita
https://www.offradio.gr/
March 9, 2022 2:53 PM


HUNCHLY
Dashboard
Capture
Case
test case
Queue 0
Selectors 0
Notes 0
Tags 0

Maltego

- Maltego is a comprehensive tool for graphical link analyses that offers real-time data mining and information gathering, as well as the representation of this information on a node-based graph, making patterns and multiple order connections between said information easily identifiable.

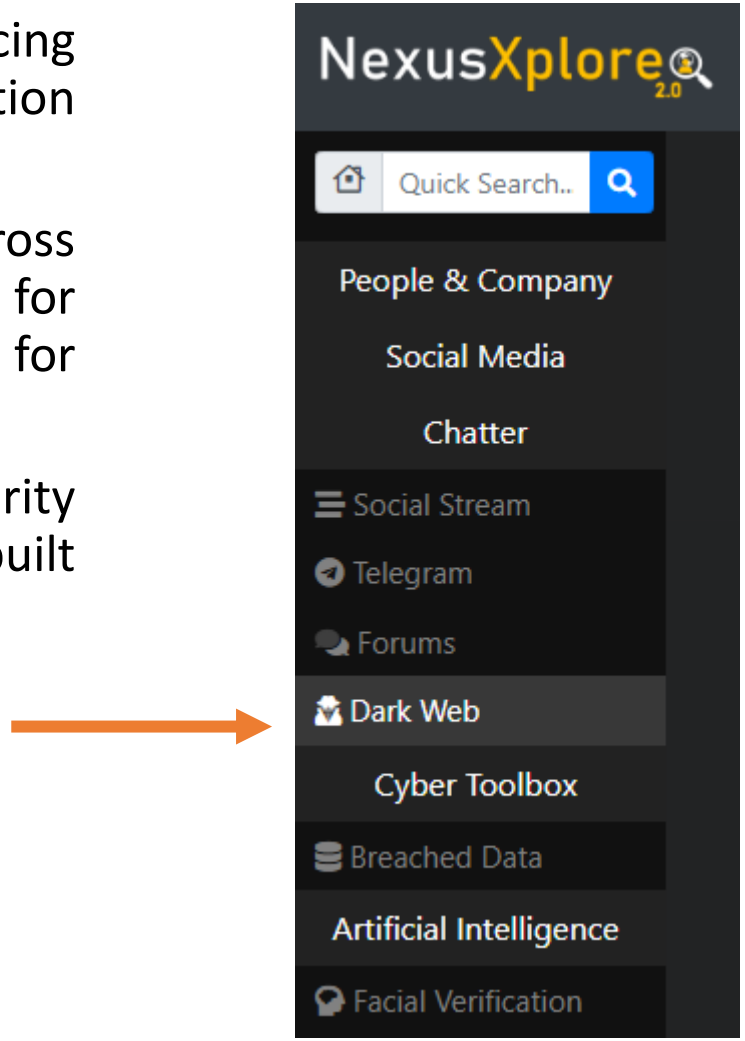


MALTEGO

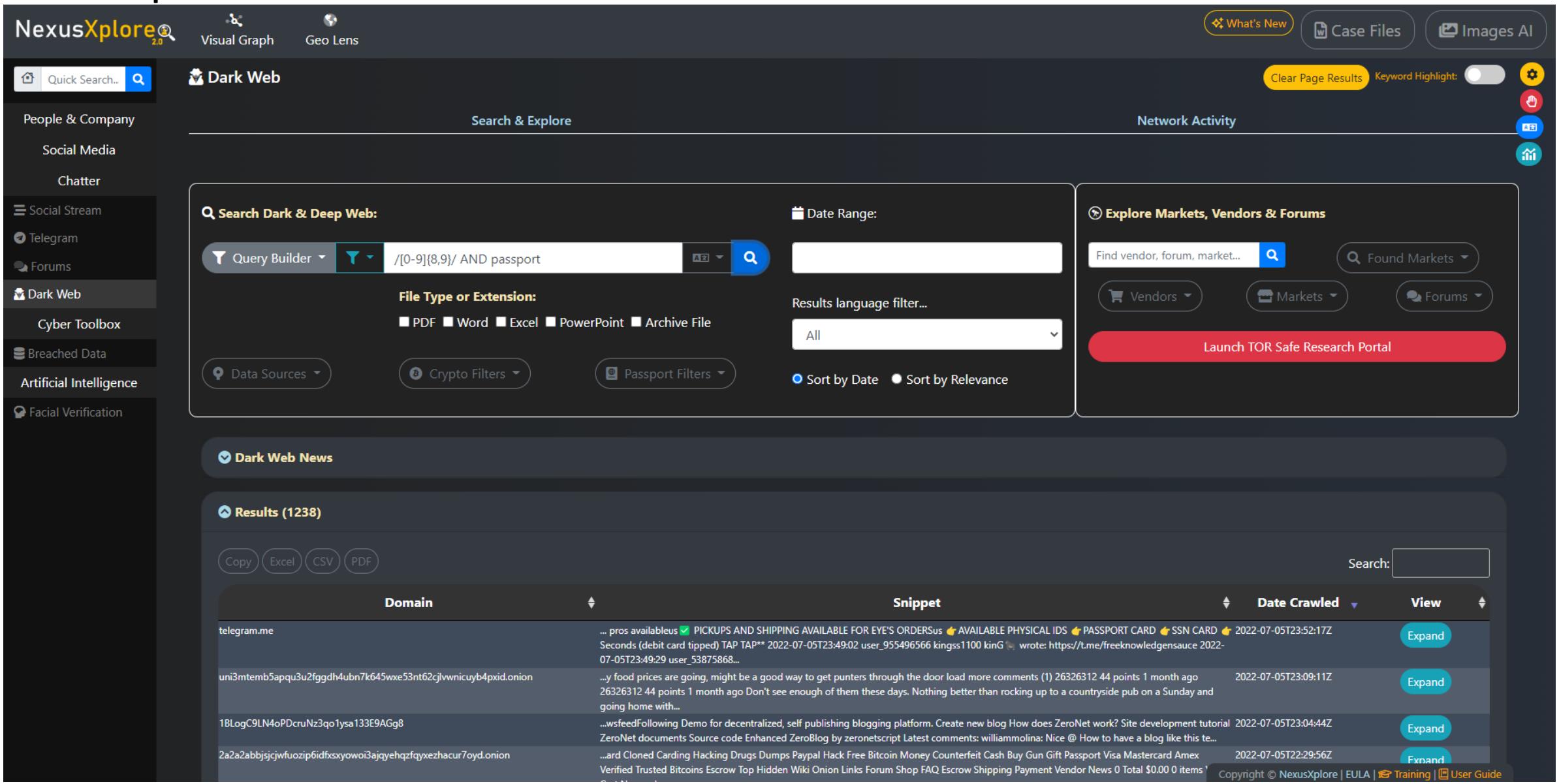
NexusXplore

- 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



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