Using OSINT Techniques to Investigate Human Trafficking and Missing Persons PT.1

JOAS ANTONIO

About PDF

- This PDF aims to show some useful techniques that can be used to investigate missing persons, victims of human trafficking or missing.

- Of course, some resources federal agencies have easy access, in addition to not being a job that anyone can do, as it requires legal issues involved

- My LinkedIn: https://www.linkedin.com/in/joas-antonio-dos-santos

- My YouTube Channel: https://www.youtube.com/channel/UCFvueUEWRfQ9qT9UmHCw_og

What is OSINT

- If you've heard the name but are wondering what it means, OSINT stands for open source intelligence, which refers to any information that can legally be gathered from free, public sources about an individual or organization. In practice, that tends to mean information found on the internet, but technically any public information falls into the category of OSINT whether it's books or reports in a public library, articles in a newspaper or statements in a press release.

- OSINT also includes information that can be found in different types of media, too. Though we typically think of it as being text-based, information in images, videos, webinars, public speeches and conferences all fall under the term.

What is IMINT

- Imagery intelligence (IMINT), pronounced as either as Im-Int or I-Mint, is an intelligence gathering discipline wherein imagery is analyzed (or "exploited") to identify information of intelligence value.[1] Imagery used for defence intelligence purposes is generally collected via satellite imagery or aerial photography.

- As an intelligence gathering discipline, IMINT production depends heavily upon a robust intelligence collection management system. IMINT is complemented by non-imaging MASINT electro-optical and radar sensors.

Human Trafficking

- Human Trafficking is the recruitment, transportation, transfer, harbouring or receipt of people through force, fraud or deception, with the aim of exploiting them for profit. Men, women and children of all ages and from all backgrounds can become victims of this crime, which occurs in every region of the world. The traffickers often use violence or fraudulent employment agencies and fake promises of education and job opportunities to trick and coerce their victims.

Investigating Techniques – Search Engine

- Search Engine Colossus
- Google
- Bing
- DuckDuckGo
- Dogpile
- ZapMeta
- MetaBear
- Exalead
- StartPage
- Swisscows
- Searx
- DisconnectSearch
- Gigablast

- Carrot2
- Wolframalpha
- Million Short
- iSeek
- eTools
- Yandex (Russia)
- Baidu (China)
- MetaCrawler (United Kingdom)
- Goo (Japan)
- Daum (Korea)
- Parseek (Iran)
- Walla (Israel)
- https://humantraffickingsearch.org/

Using Search Engine – Internet Search

- Known as DIG (for Domain-specific Insight Graphs), the tool allows officers who are searching for a missing child who is believed to be trapped in the escort industry to search by phone number, location, alias — even by photo — and pin down a way to reach them.

- "The Internet contains seemingly limitless information, but we're constrained by our ability to search that information and come up with meaningful results. DIG solves that problem," said Szekely, research associate professor at ISI.

- DIG is simple enough that it won't require special training to use. The database it utilizes currently has 50 million Web pages, 2 billion records and grows at a rate of roughly 5,000 pages per hour.

Using Search Engine – Internet Search 2

- The funding and initiative to create DIG came from Memex, a Defense Advanced Research Projects Agency (DARPA) program aimed at developing the next generation of Internet search tools in hopes of helping law enforcement agencies fight online human trafficking.

- The code for DIG is open-source — and therefore free to law enforcement agencies — and will be upgraded quarterly over the course of the three-year project, which began in 2014. For example, Szekely and Knoblock plan to improve DIG so that it automatically flags potential victims and identifies trafficking rings through their ads and the victims under their control.

- https://news.usc.edu/81360/internet-search-tool-takes-on-human-traffickers/

GEOINT

- GEOINT is the use of location- and time-based data to create maps and other forms of geographically plotted information, such as traffic on shipping routes. GEOINT can be used to identify customer distribution, help farmers maintain soil health, and plan for emergency preparedness. GEOINT has been transformed using cloud computing, allowing powerful Machine Learning (ML) algorithms to be applied to a wide variety of data. Maps and other reports can be created quickly to reveal underlying patterns at a glance.

- OSINT- and GEOINT-based techniques can be used for a wide variety of tasks, but they both have areas of unique utility. OSINT-based techniques are particularly good at taking small, unrelated pieces of information and extracting the truths behind them. GEOINT-based techniques are particularly good at correlating large amounts of data in space and time in a way that allows broader patterns to emerge.

Investigating Suspect – Sock Puppet

- Sock puppets are nothing but detailed created fake social media accounts to research in OSINT without giving up the true identity.

- Sock Puppets are basically aliases, fictitious persona profiles created by someone else with specific goals in mind and is part of an OSINT Social Engineering technique.

- These type of accounts can be used by anyone like investigators, detectives, hackers, police, journalists, it can be anyone who wants to impersonate someone else.

Investigating Suspect – Purpose of Sock Puppet

- Sock puppets can be used in various different ways:
  1. Investigators can use the sock accounts to collect information and do research o some cases.
  2. Hackers can use sock accounts to do social engineering on the target to collect the information.
  3. Detective can use these type of accounts to collect information and to know the nature of someone related to their cases.
- Basically, sock accounts are used to collect information or to look into someone without letting them know. Anyone can use it in anyway they like.

Investigating Suspect – Create Sock Puppet 1

- Fake Name Generator

https://www.fakenamegenerator.com/

https://www.elfqrin.com/fakeid.php

https://www.4devs.com.br/

From fake name generator you can create a person that never have existed with Name, address, mother's Maiden name, Address, Email address, weight, height, credit card, date of birth, favorite color, vehicle number and all sorts of information you need to be that person.

Investigating Suspect – Create Sock Puppet 2

- Email providers

  Gmail.com

  Yahoo mail

  Proton Mail

  Outlook.com

  Mail.com

- I recommend using mail.com to create email address and make sure you don't use existing email address.

Investigating Suspect – Create Sock Puppet 3

- Now we need a face for image verification

- https://thispersondoesnotexist.com/

- You can get a face from the above link just refresh the website until you are satisfied with your face.

- This website create fake faces with AI so the faces created by the website do not exists in real world. so you can be one.

- Now we have all the important ingredients to create account

- (thispersondoesnotexist.com) – GitHub project available

- AI Generated Faces (boredhumans.com)

- Gallery of AI Generated Faces (generated.photos)

Investigating Suspect – Create Sock Puppet 4

- Creating an account can take some time, effort, and creativity. If you are short on any of those for whatever reason. Anyone that has played roll playing games like D&D, WARHAMMER, or other games where you need to generate a character to play, has a step up because they have done this before. There are a few resources you can leverage to help speed up the process and spit out a "character" with a lot of random attributes and content. Below is a list of resources you can use when generating your Sock Puppet persona. Just remember that all information generated is fake. You can change the data to fit your narrative:

- Fake Identity Generator (fakepersongenerator.com)

- Random Name Generator (www.elfqrin.com/fakeid.php)

- Random Character Generator (random-character.com)

- Personality Generator (rangen.co.uk)

- Trait Generator (rangen.co.uk)

Investigating Suspect – Create Sock Puppet 5

- **Burner Phones**

- A burner phone is extremely useful and may be required to create accounts on certain websites along with creating a history for the persona. The reason is the sites are trying to prevent fake accounts from being created and will send an SMS validation message to a phone. Bots rarely have their own phone numbers. In some countries, you do not need to tie your ID or Passport to buy a SIM card or burner phone. If you are in one of these countries, it is suggested to use cash only and let the phone sit for 2+ months before you activate it with a sock puppet email. Sometimes SIM cards can also be purchased on Amazon.com. Keep an eye out for deals and trial offers. Phone emulators can also work.

- **VoIP Phone**

- Generate a Voice over IP (VoIP) account with an online vendor. This will be useful to add another layer of separation. Many of the online services like Google Voice require you to have a real phone number to tie to your account. This makes your burner phone that much more important.

Investigating Suspect – Create Sock Puppet 6

- **Cryptocurrencies**

- If your investigation requires cryptocurrencies for transactions, you can use prepaid cards on most of the crypto services. Exodus.com is a wallet that allows you to trade many different currencies and their Desktop software is cross platform compatible. An example of needing crypto currencies during an investigation may include fraud cases on sites like Facebook Marketplace, Instagram's Shop Now, Craigslist, etc. You may also find them useful when purchasing content and buying services.

Investigating Suspect – Create Sock Puppet 7

- **Social Media Accounts**

- When creating a social media account, you want to look as 'normal' as possible to the website because many of them are trying to stop people from creating fake accounts. Make sure you are not breaking the law or violating terms of service when doing this. Now things to look at when creating your OSINT undercover accounts:

- Use public Wi-Fi and do NOT use a VPN

- Pick a social media site to focus on

- Use your persona's "real" phone number for verification

- Save the information in a password manager like KeePassXC

- Keep Operational Security (OPSEC) in mind:

- Use a very strong password for the password manager access

- Use a different password for each account

- Never cross over accounts with your real world or personal accounts

- Go into the settings of the account you just created and change the phone number to a VoIP number

- When you are done, log out of the account

- Log back in and start adding information to your account relevant to the profiles

- Go back to step 2 for the rest of the sites you want to try

https://csilinux.com/blog/Using-Sock-Puppet-Accounts-for-OSINT/

Reverse Image Search

- Reverse image searches are an important part of any OSINT investigation. There are dozens of specialist search engines available, each with its own strengths and weaknesses, but checking an image against numerous separate search engines is time consuming.

- https://github.com/Brawl345/Image-Reverse-Search-WebExtension

- https://smallseotools.com/reverse-image-search/

- https://tineye.com/

Metadata Image Osint

- Image metadata is text information pertaining to an image file that is embedded into the file or contained in a separate file that is associated with it.

- Image metadata includes details relevant to the image itself as well as information about its production. Some metadata is generated automatically by the the device capturing the image. Additional metadata may be added manually and edited through dedicated software or general image editing software such as GIMP or Adobe Photoshop. Metadata can also be added directly on some digital cameras.

- Image metadata can be very useful for cataloging and contextualizing visual information. Many visual artists find the features useful in providing data about themselves and their images.

- Image metadata can also help protect Intellectual property. It is important to note, however, that copyright information is not adequate protection as it can easily be stripped away. Also, as with other types of content, metadata security can be cumbersome, requiring extra measures to secure image metadata and protect it from unauthorized access.

Metadata Image Osint – tools

- https://jimpl.com/

- https://www.metadata2go.com/

- https://brandfolder.com/workbench/extract-metadata

- https://www.youtube.com/watch?v=d3NsT8lJRlE&ab_channel=Bendobrown

- https://www.youtube.com/watch?v=UgtE_hoLCDY&ab_channel=ehacking

Investigate Social Media Profile

- Lookup-id.com
- Sowdust
- Facebook Matrix
- Facebook Graph Searcher
- Facebook Graph, Codes & Operators
- Iconosquare
- Socialrank
- Teaching Privacy
- Search My Bio
- Twitter Advanced Search
- Twitter Search Tricks
- Twitter Directory
- Tweet Deck
- TweeterID
- GetTwitterID
- TweetBeaver
- Socialbearing
- Onemilliontweetmap

- Followerwonk
- Herdlocker
- Keyhole
- Twiangulate
- Twitterfall
- Twipho
- Trendsmap
- Mentionmapp
- TinfoLeak
- Twlets
- Tweetarchivist
- Sleeping Time
- Spoonbill
- First Tweet

Social Media Osint, also known as Social media intelligence allows one to collect intelligence gathering from social media sites like Facebook, Twitter, Instagram etc. This type of intelligence gathering is one element of OSINT (Open- Source Intelligence).

https://github.com/InfuriousICC/Social-Media-Osint
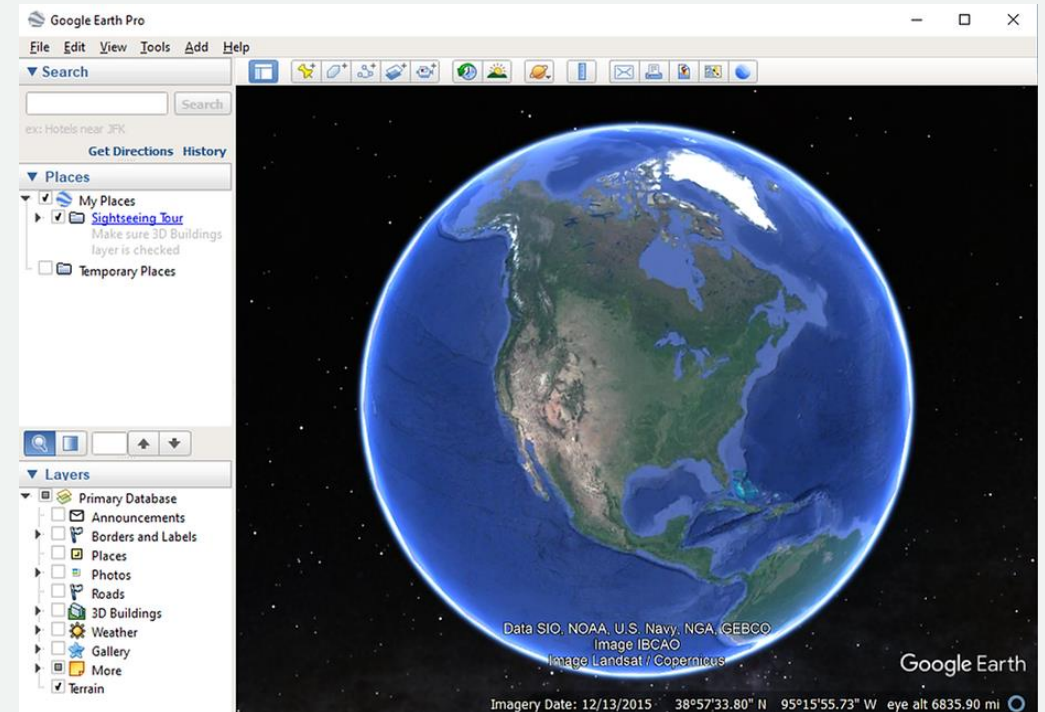
Investigate Social Media Profile 2

- Static information provided about a specific user that is observable by those who access the profile. On LinkedIn, for instance, this might include a user's job title, current and former employers, skills, and contact information.

- Users on a social media platform can interact with the platform or other users in many ways. These forms of interaction include posting/commenting, replying to someone else's content, posting pictures or videos, and liking or reacting to existing content.

- Information found on social media platforms is not limited to text and pictures. It can also include contextual information about said pieces of content. Metadata can include the location tagged in a post, the time that the post was made, or even the type of device used to take a picture.

- https://www.youtube.com/watch?v=FceN0T_a_uM&ab_channel=PatervaMaltego

Investigate Social Media Profile 3

- Static information provided about a specific user that is observable by those who access the profile. On LinkedIn, for instance, this might include a user's job title, current and former employers, skills, and contact information.

- Users on a social media platform can interact with the platform or other users in many ways. These forms of interaction include posting/commenting, replying to someone else's content, posting pictures or videos, and liking or reacting to existing content.

- Information found on social media platforms is not limited to text and pictures. It can also include contextual information about said pieces of content. Metadata can include the location tagged in a post, the time that the post was made, or even the type of device used to take a picture.

- https://www.youtube.com/watch?v=FceN0T_a_uM&ab_channel=PatervaMaltego

Google Maps OSINT

- https://www.hackers-arise.com/post/open-source-intelligence-osint-using-google-earth-pro-satellite-imagery-for-investigations

- https://www.youtube.com/watch?v=n_kJJXoLo8I&ab_channel=TheOSINTCuriousProject

- https://www.youtube.com/watch?v=54XwmS-fi-A&ab_channel=0x4rk%C3%98

- https://www.osintessentials.com/maps

- https://nixintel.info/osint-tools/three-useful-resources-for-maps-and-satellite-images/

OSINT Framework

- OSINT framework focused on gathering information from free tools or resources. The intention is to help people find free OSINT resources. Some of the sites included might require registration or offer more data for $$$, but you should be able to get at least a portion of the available information for no cost.

- I originally created this framework with an information security point of view. Since then, the response from other fields and disciplines has been incredible. I would love to be able to include any other OSINT resources, especially from fields outside of infosec. Please let me know about anything that might be missing!

- https://osintframework.com/

Public Records Search

- Although public record is the common term used to refer to data that is publicly accessible, it also goes by the name OSINT. OSINT stands for Open-Source Intelligence, which is data from publicly available sources. Data like this used to come from newspapers and other publications but now, they can also be gathered via public social media posts such as Twitter, Facebook, and Instagram. With this said, it should be noted that the availability of data is not just about tech but also about the strategy used by private investigators. It pays to know where to look and know how to filter data to gather only the most relevant for an investigation.

Public Records Search

- **Why Use Public Records to Gather Intelligence?**

- Information is expensive and not easily available for a lot of people. The beauty of using public records to gather intelligence is that it makes things faster, more efficient, cheaper, and easier because of the following:

- It is cost-effective. You get highly-valuable information for less effort so that each piece of information comes cheaper or at least worth every penny. For example, finding out that a potential business partner is a scammer can save you time, money, and the headache of finding out later.

- It provides legitimate and reliable data. Using public records to investigate means that information can be easily verified and thus, is legitimate and reliable. By using public records, you can easily check on someone?s identity, claims of achievement, employment history, and more whilst being perfectly legal.

- Public records often point to other useful data sources. For example, if you find out that someone served in the military via a publicly recorded source, then you would know what is the next step to take and where to look for further information.

- It is discreet. An investigation can be completed just by using public records. This means that there will be no surveillance needed, no need to interview people, and nearly everything can be done online in secret.

- Public records make it easier to see discrepancies and biases. Some pieces of information are only recorded to support certain agendas. This may not be easy to figure out if things are all private but when things are publicly accessible, it can be easy to see patterns that point towards a bias.

https://haywoodhunt.ca/understanding-osint-and-the-power-of-public-records/
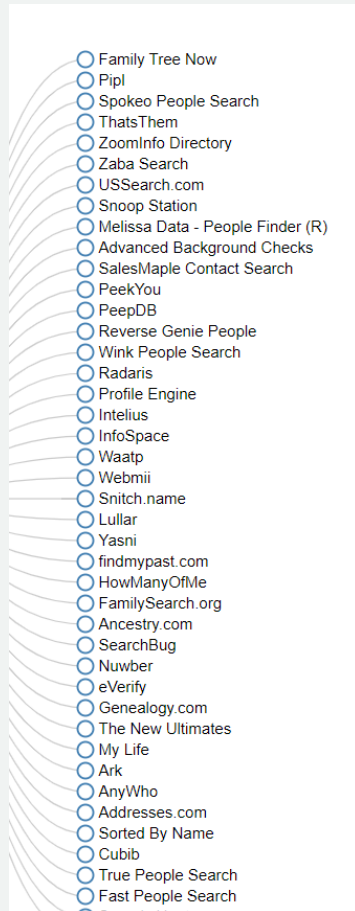
Public Records Search 2

- Information is expensive and not easily available for a lot of people. The beauty of using public records to gather intelligence is that it makes things faster, more efficient, cheaper, and easier because of the following:

- It is cost-effective. You get highly-valuable information for less effort so that each piece of information comes cheaper or at least worth every penny. For example, finding out that a potential business partner is a scammer can save you time, money, and the headache of finding out later.

- It provides legitimate and reliable data. Using public records to investigate means that information can be easily verified and thus, is legitimate and reliable. By using public records, you can easily check on someone?s identity, claims of achievement, employment history, and more whilst being perfectly legal.

- Public records often point to other useful data sources. For example, if you find out that someone served in the military via a publicly recorded source, then you would know what is the next step to take and where to look for further information.

- It is discreet. An investigation can be completed just by using public records. This means that there will be no surveillance needed, no need to interview people, and nearly everything can be done online in secret.

- Public records make it easier to see discrepancies and biases. Some pieces of information are only recorded to support certain agendas. This may not be easy to figure out if things are all private but when things are publicly accessible, it can be easy to see patterns that point towards a bias.

https://haywoodhunt.ca/understanding-osint-and-the-power-of-public-records/

https://www.youtube.com/watch?v=F5DaPt4W5Oo&ab_channel=SANSCyberDefense

Public Records Search 3

- Family Tree Now
- Pipl
- Spokeo People Search
- ThatsThem
- ZoomInfo Directory
- Zaba Search
- USSearch.com
- Snoop Station
- Melissa Data - People Finder (R)
- Advanced Background Checks
- SalesMaple Contact Search
- PeekYou
- PeepDB
- Reverse Genie People
- Wink People Search
- Radaris
- Profile Engine
- Intelius
- InfoSpace
- Waatp
- Webmii
- Snitch.name
- Lullar
- Yasni
- findmypast.com
- HowManyOfMe
- FamilySearch.org
- Ancestry.com
- SearchBug
- Nuwber
- eVerify
- Genealogy.com
- The New Ultimates
- My Life
- Ark
- AnyWho
- Addresses.com
- Sorted By Name
- Cubib
- True People Search
- Fast People Search

Using public database, it helps you to search important information about a certain person.

There are many leaks of addresses too, which is used as an addition in an analysis and intelligence to obtain information from people, because a kidnapper or someone missing does not escape having their data leaked at some point.

OSINT for Missing Persons

- https://mchughsecurity.com/2020/04/10/osint-for-missing-persons-part-1-intro/

- https://www.youtube.com/watch?v=rrUFjUTMsfg&ab_channel=0x4rk%C3%98

- https://www.youtube.com/watch?v=4lv8Th6gZM4&ab_channel=BSidesVancouver

- https://www.youtube.com/watch?v=34VbLCqhdrs&ab_channel=GeraldAuger%2CP
  hD-SimplyCyber

- https://www.youtube.com/watch?v=RIZxrfqMwVE&ab_channel=GeraldAuger%2CP
  hD-SimplyCyber

- Something many investigators do is create a pattern, using maps like google maps
  itself, to draw a disappearing line.

OSINT for Missing Persons 2

- Here is a simple example, I used any address and made a triangulation, based on the mapped points, to get an idea of the modus operandi. Not meaning that the victims can be in the same place, sometimes they are not even in the state anymore, but it is a beginning for investigation and understanding why these points are the most interesting.

- Details: I used any address

- https://www.youtube.com/watch?v=2puBmXfi9Z0&ab_channel=Freethink

Investigate Human Trafficking OSINT

- Investigate job ads and classifieds, many sites contain fake ads for malicious purposes

- These same ads are posted all over the States and Europe mostly using fake photos without any phone number. And if the number is listed, it is used on different sites and for different cities so I strongly believe it's also fake. You can just google number but remember to put it in quotes for exact search.

- https://www.youtube.com/watch?v=ero94P8mEto&ab_channel=UCBerkeley

- https://www.offensiveosint.io/offensive-osint-s01e08-human-trafficking-investigation-part-1/

- https://www.youtube.com/watch?v=mlURFD15Uic&ab_channel=GlobalInvestigativeJournalismNetwork

Investigate Human Trafficking OSINT 2

- Many Backpage and Ad-focused sites in general are the most likely to roll human traffic, but there is a huge icerberg to get to deeper layers.

- Social networks can become a vector for this type of action, especially with the recruitment of people for jobs with interviews scheduled in totally suspicious physical locations.

- https://www.osha.gov/pls/imis/establishment.html

- https://www.melissa.com/v2/lookups/addresssearch/

- https://www.pocket-lint.com/apps/news/156660-address-lookup

- Search for information on a specific address and see who owns the place, in addition to the existence of a company registered in that place. A lot of the time, some places are just made as a shell company to carry out fake interviews and others.

Google Maps Crime Solved – Missing Person

- https://www.youtube.com/watch?v=LcgK-WV4Z4I&ab_channel=VICE

- https://www.youtube.com/watch?v=x724A8eN8A8&ab_channel=CrimeZone

- Many use their free time to scour google maps, however it often happens that they find something strange, like someone missing, for example, or even solve a crime for years.

- Some map addresses where the disappearance occurred and use Google Maps to see if they can find anything.

Additionals Websites

- https://www.fbi.gov/how-we-can-help-you/victim-services
- https://www.youtube.com/watch?v=bVEjXT5t_Gc&ab_channel=TrueCrimeDaily
- https://www.youtube.com/watch?v=jHcoEY6gJJ0&ab_channel=RebeccaBenderInitiative
- https://www.youtube.com/watch?v=fNzqknAjPDc&ab_channel=LAcrimestoppers
- https://www.justice.gov/opa/pr/fbi-announces-results-nationwide-sex-trafficking-operation
- https://humantraffickinghotline.org/es/report-trafficking
- https://www.cdss.ca.gov/reporting/report-abuse/report-human-trafficking
- https://www.met.police.uk/ro/report/mp/v2/report-missing-person/
- https://www.missingpeople.org.uk/get-help/help-services/how-police-search/how-to-report-someone-missing
- https://www.gov.uk/report-missing-person
- https://www.youtube.com/watch?v=O1EkZK6ChIk&ab_channel=RealStories
- https://www.youtube.com/watch?v=Pb7x0RveNzU&ab_channel=ColdCaseDetective

Awesome OSINT

- https://github.com/jivoi/awesome-osint

- https://github.com/lorien/awesome-osint

- https://github.com/priyankvadaliya/AwsomeOSINT

- https://www.tracelabs.org/initiatives/osint-vm