Usando OSINT para investigar Tráfico Humano e pessoas desaparecidas
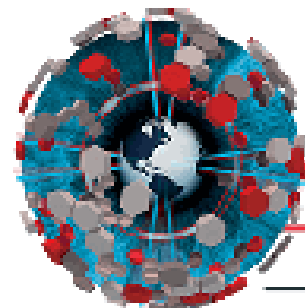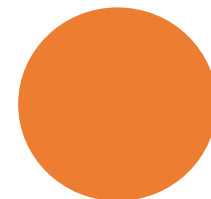
H2HC

HACKERS TO HACKERS CONFERENCE

Whoami

- Red Team Leader, PenTester, Instrutor;

- Possui algumas CVE's publicadas;

- Contribuidor do Mitre Att&ck;

- +90 Certificações internacionais;

- Contribuidor do Hacking is Not a Crime;
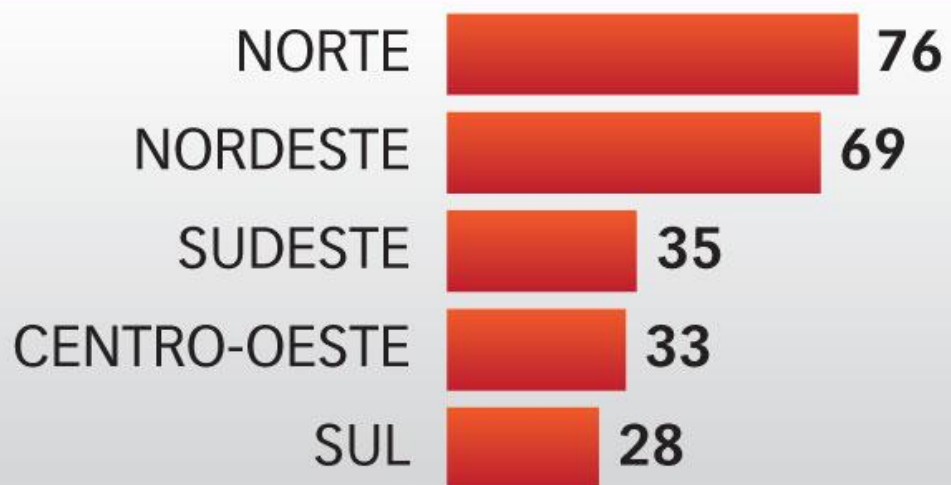
- Synack Red Team Member;

- Autor e Palestrante;

ROTAS DE TRÁFICO DE PESSOAS

Região	Valor
NORTE	76
NORDESTE	69
SUDESTE	35
CENTRO-OESTE	33
SUL	28

Fonte: Centro de Referência, Estudos e Ações sobre Crianças e Adolescentes

Cerca de 63 mil pessoas desapareceram no último ano no Brasil. Como reagem as famílias?

O desaparecimento de pessoas é um problema coletivo, gera ambiguidade e desgasta a saúde física e mental de familiares que buscam entes desaparecidos
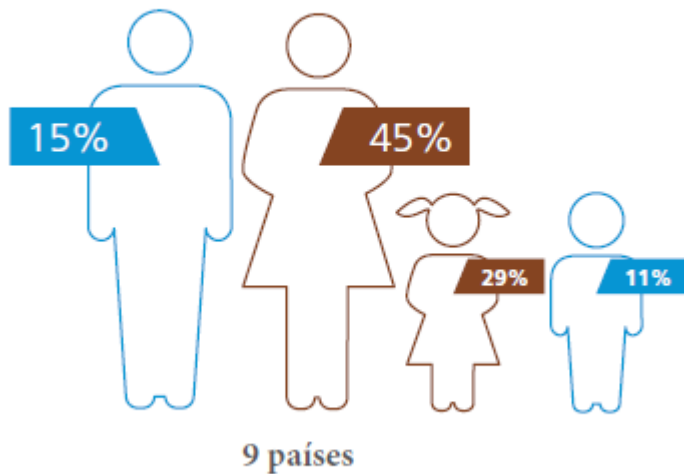
21 million - 45 million

the estimated number of people trapped in some form of slavery

END SLAVERY NOW

victims of human trafficking

Vítimas de tráfico detectadas na América do Sul, por gênero e idade, 2014 (ou mais recente)

15%   45%   29%   11%

9 países

Fonte: UNODC - elaboração de dados nacionais

PREVENÇÃO AO TRÁFICO DE PESSOAS:

DEIXE ENDEREÇO, TELEFONE E/OU LOCALIZAÇÃO DA CIDADE PARA ONDE ESTÁ VIAJANDO

ANTES DE ACEITAR QUALQUER PROPOSTA, PESQUISE SOBRE O CONTRATANTE

DUVIDE SEMPRE DE PROPOSTAS DE EMPREGO FÁCIL E LUCRATIVO

SINAIS DE QUE A PESSOA ESTÁ SENDO VÍTIMA:

PASSAPORTE OU DOCUMENTOS DE VIAGEM NA MÃO DE TERCEIROS

NÃO CONHECEM O ENDEREÇO DA CASA PARA ONDE VÃO OU DO LOCAL DE TRABALHO

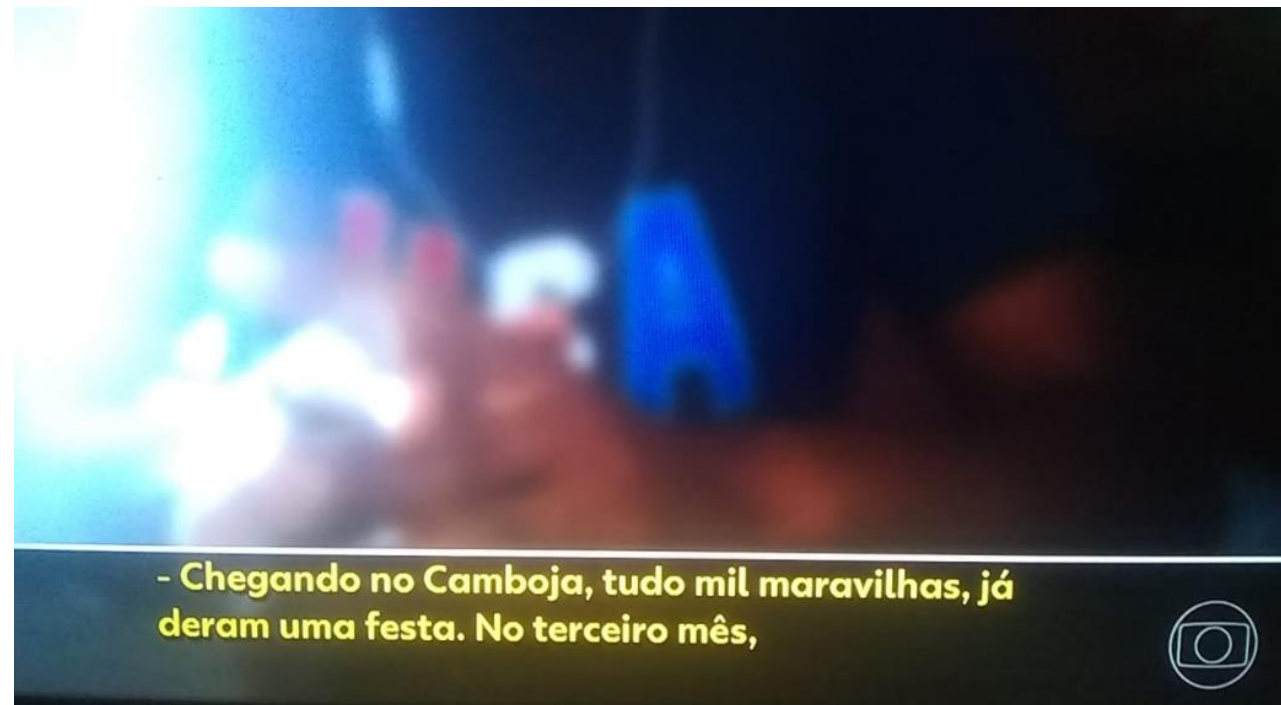FALAM POUCO OU NÃO FALAM COM OS FAMILIARES E AMIGOS

EM CASO DE DESCONFIANÇA, DISQUE 100 OU LIGUE 180

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA

PÁTRIA AMADA BRASIL
GOVERNO FEDERAL

H2HC
HACKERS TO HACKERS CONFERENCE

victims of human trafficking #2

TRÁFICO DE PESSOAS
Brasileiros denunciam que viviam em cárcere privado no Camboja

- Chegando no Camboja, tudo mil maravilhas, já deram uma festa. No terceiro mês,

What is OSINT?

- OSINT stands for open source intelligence, which refers to any information that can be legally collected from free public sources about an individual or organization;

- It means information found on the internet, but technically any public information falls under the OSINT category;

What is IMINT?

- Image intelligence (IMINT), is an intelligence collection in which images are analyzed to identify information that generates intelligence value;

- As an intelligence collection discipline, IMINT production relies heavily on a robust intelligence collection management system;
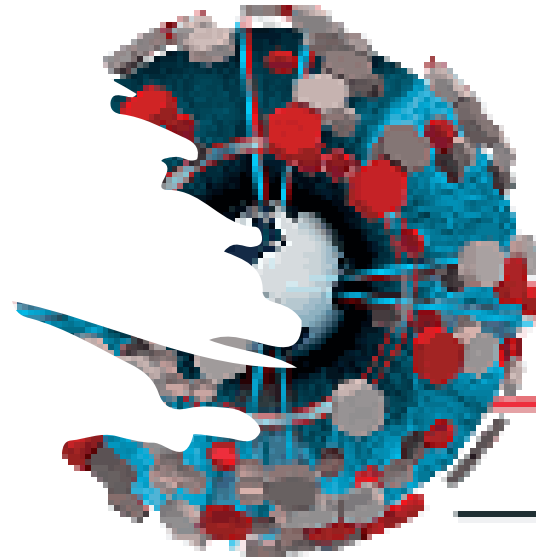
about human trafficking

- Trafficking in persons is the recruitment, transportation, transfer, harboring or reception of persons through force, fraud or deception, with the aim of exploiting them for profit.

Research search engines

- The internet contains a wealth of information that is useful for an investigation of human trafficking or missing persons;

- 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)

Research search engines #2

- Use of Google dorks and advanced search operators;

- Search employment agency websites, ads and classifieds;

- Map fake websites;

- Search for addresses and information about people;
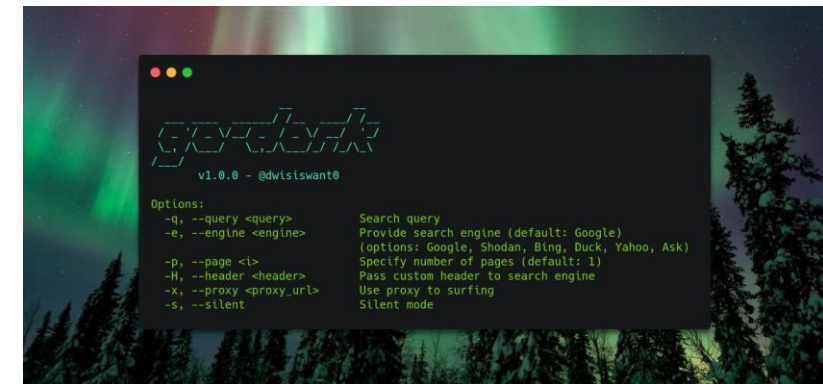
Social networks in research

- Social networks are a rich source of information;

- Collect information about a particular person or company;

- Include contextual information about said contents. Metadata can include the location tagged in a post, the time the post was made, or even the type of device used to take a photo;

Social Media Resources

Facebook
- Lookup-id.com
- Sowdust
- Facebook Matrix
- Facebook Graph Searcher
- Facebook Graph, Codes & Operators

People Search Engines
- Family Tree Now
- PeekYou
- That'sThem
- Qwant
- Webmii
- ZabaSearch
- FastPeopleSearch
- Radaris
- Intelius
- Yasni
- iTools
- Canada 411
- 192 UK Search

Twitter
- 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

YouTube
- YouTube GeoFind
- YouTube Metadata
- Geo Search Tool
- YouTube DataViewer
- InVID Verification Plugin
- Yasiv
- Yout
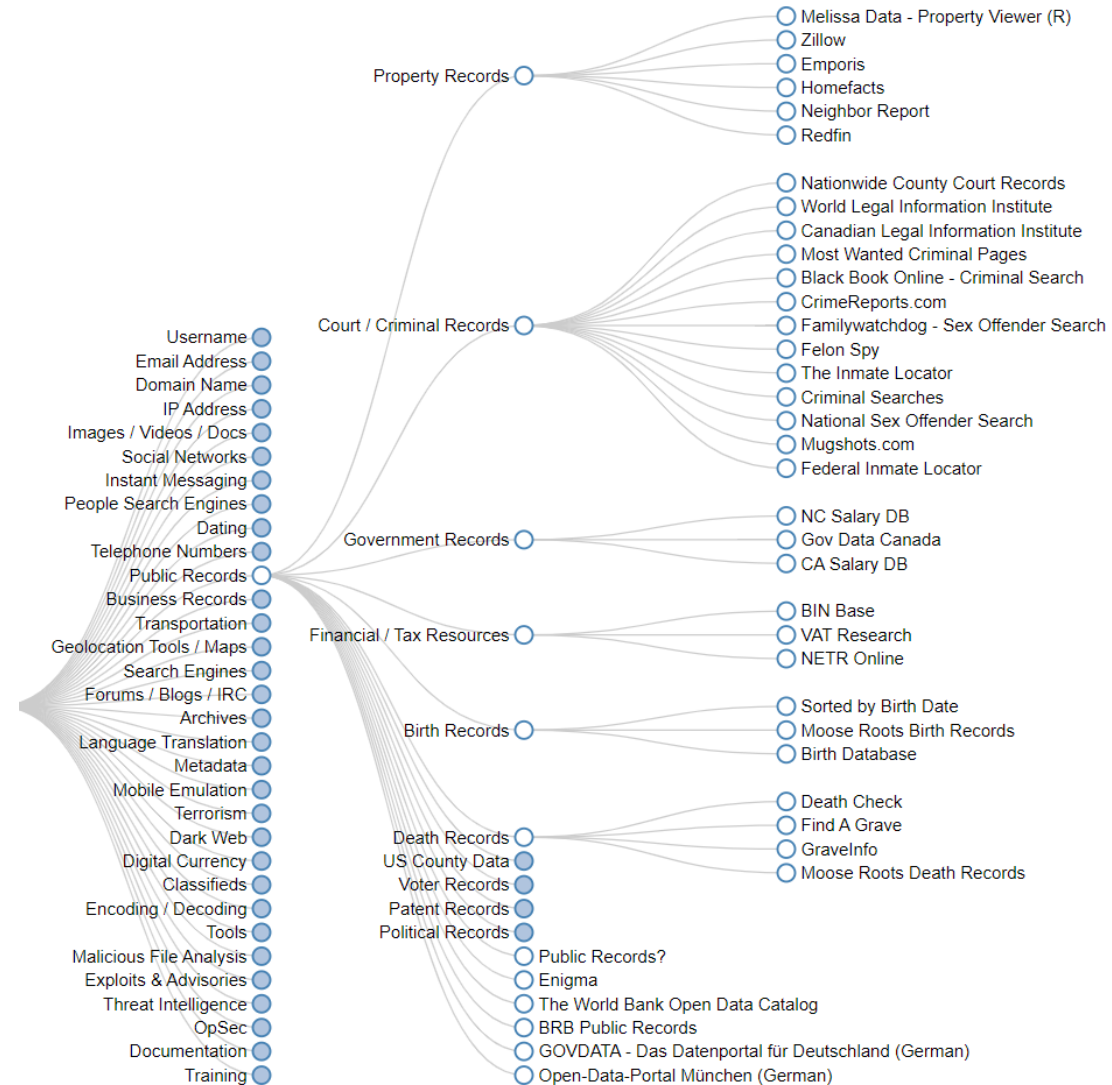- TubeChop
- Deturl
- Watchframebyframe
- Savefrom
- Y2mate
- Keepvid

Instagram
- Iconosquare
- Socialrank
- Teaching Privacy
- Search My Bio

Snapchat
- Snap Maps
- Snapchat Username

Public Information Search

- Using the internet to collect information about a person;
- Address, telephone, personal information, etc.;

Public Information Search #2

- There are online telelists that help in looking up telephone numbers by address;

- And websites that we can use to look up a specific address;

- In addition to data house which is used by criminals to obtain information about a person;
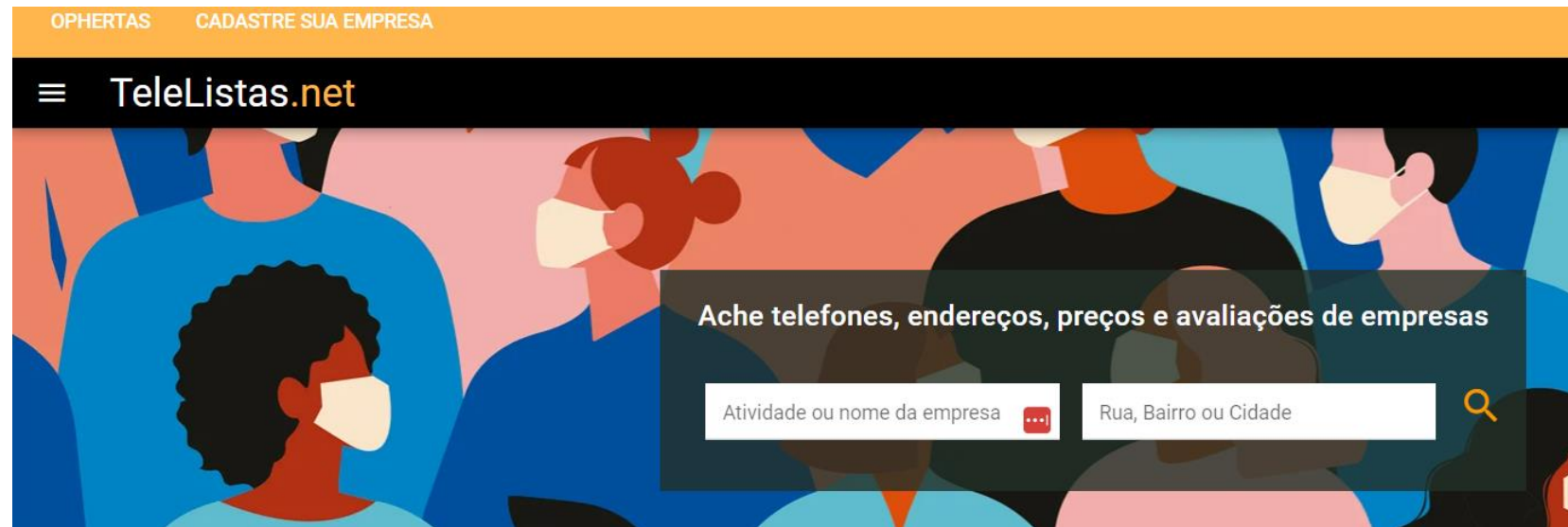
Public Information Search #3

- Data leaks are often used in an OSINT investigation;

- Leakage of addresses, telephone numbers, documents and others;
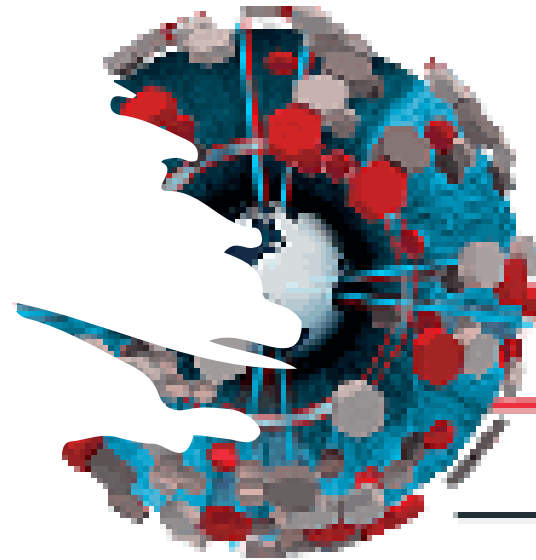
August 8, 2022, 05:46 PM (This post was last modified: September 21, 2022, 03:13 AM by bash.)

Warning: Before you decide to buy, read the entire thread:

This leak is semi-private, some people may have it, or there may be inferior versions with less data or incomplete dat

Some people have already announced this here but the overwhelming majority are just scammers or someone who i Experian.

With these considerations in mind and since you at Breached deserve the best, I'm selling the 1.8TB version of Seras

Leak details:
- Data is up to 03 February 2020.
- The file format is a .bak weighing 464.04GB (you will restore it in SQL SERVER and once the backup is restored the
- The leak has 119 tables
- The number of records of each table and the size of each table will be attached below.
- This leak has over 158 million unique emails and data from over 233 million Brazilians.

Contact:
- Jabber: handrail0219@xmpp.jp
- QTOX: DB8169DA4FCFAE036DCEB5A44A4DF0994D06DFDAF2756081F586C2A76A23283258B0D761CBE0
- TELEGRAM: @handrail0219 (I created it using a temporary number, if my account is deleted and we are in the midd here.)
- Or you can send me a private message

Creating a sucket puppet for investigation

- Creating a fake account is not just for illicit use, but useful for an investigation without putting your identity at risk;
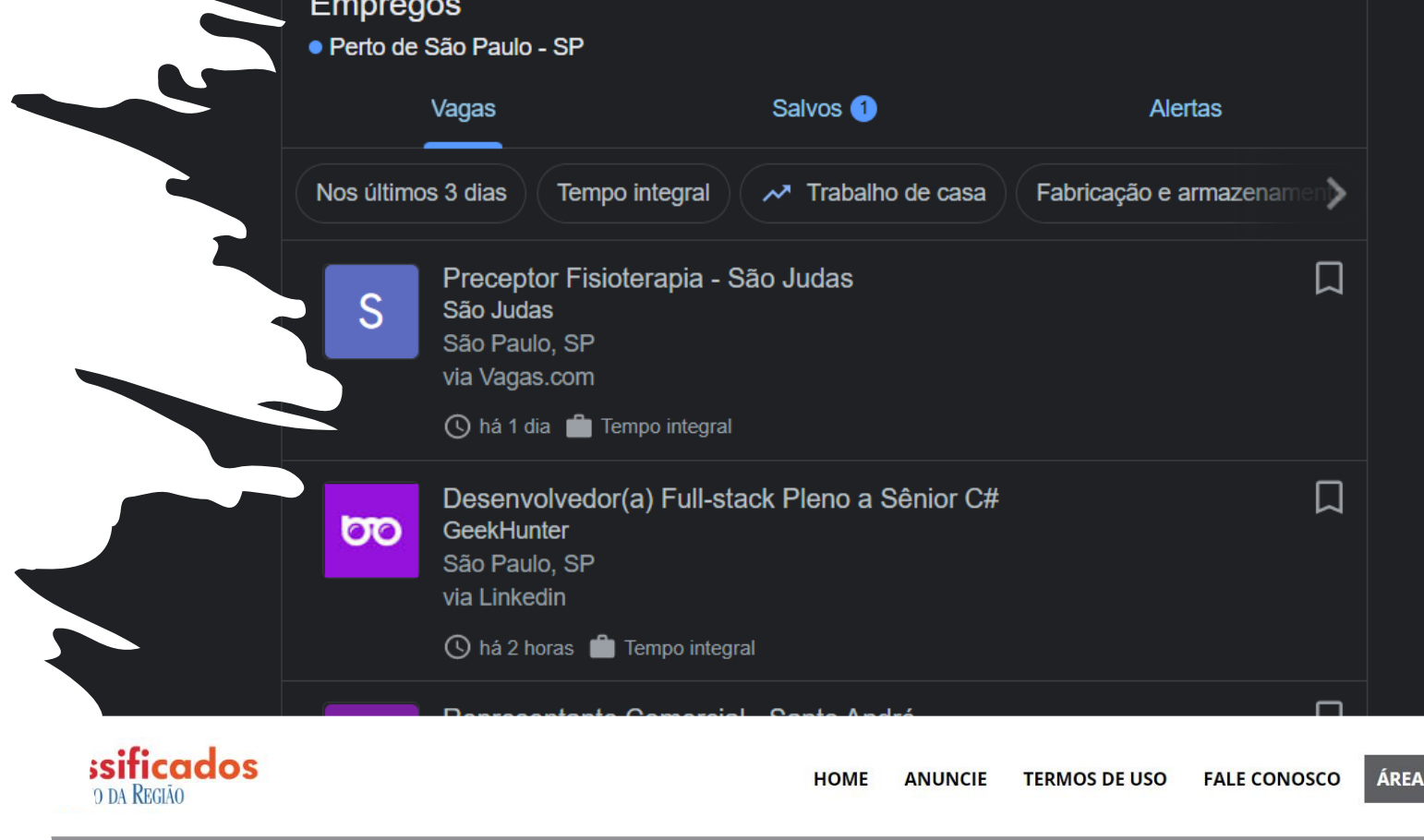
Useful techniques:
- Generate a name, address and fake documents;

https://www.4devs.com.br/
- Create a fake email for use;

Gmail.com

Yahoo mail

Proton Mail

Outlook.com

Mail.com
- Using a fake profile picture;

https://thispersondoesnotexist.com/
- Use an alternative phone number to receive SMS and call;

Investigating human trafficking #1

- Investigating job sites and classifieds can give a sense of the modus operandi of criminals;

- Many use a fake vacancy, with a phantom address and a phantom selection process;

- Promise of on-the-job training or travel;

- Additionally, classifieds sites are used to advertise job openings or other opportunities;

Investigating human trafficking #2

- Ads on walls or poles are a great gimmick;

- In addition to social networks such as Tinder, Instagram or Facebook, mainly for grooming and false promises;

- Using profile fakes and friendly approaches to win over victims, even using oranges for that purpose;
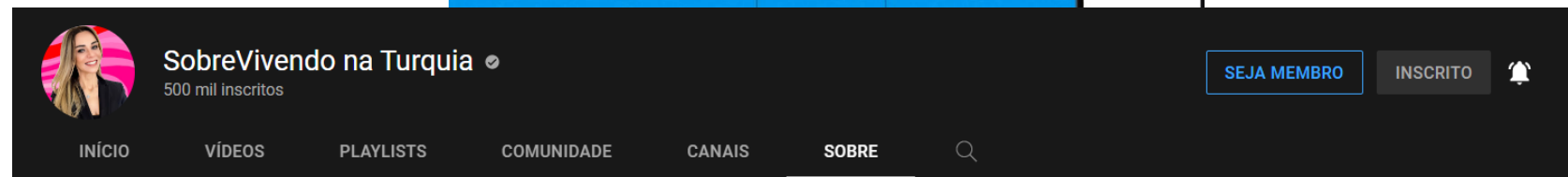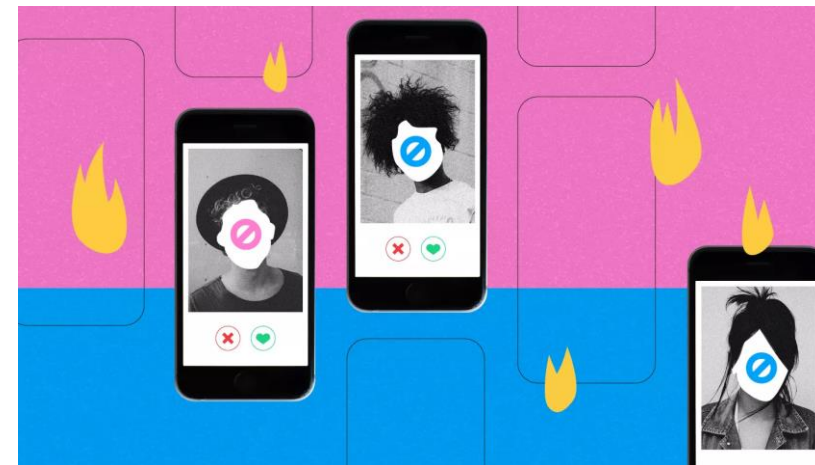
Useful techniques for investigating missing persons

- Example of triangulation to define a research strategy;

- Crimes have already been solved using Google Maps itself;

- A very useful tool is Seeker, which collects geolocation by creating a fake URL;

Useful techniques for investigating missing persons #2

- The metadata of an image is useful for an investigation, especially if the missing victim posted a photo hours earlier;

- Reverse image searches are an important part of any investigation to find the real source of a given image;

Reverse Image

- Google Images
- Bing Images
- Yandex Images
- Baidu Images
- Tineye
- Image Identify by Wolfram
- Karma Decay
- Pictriev

Image Metadata
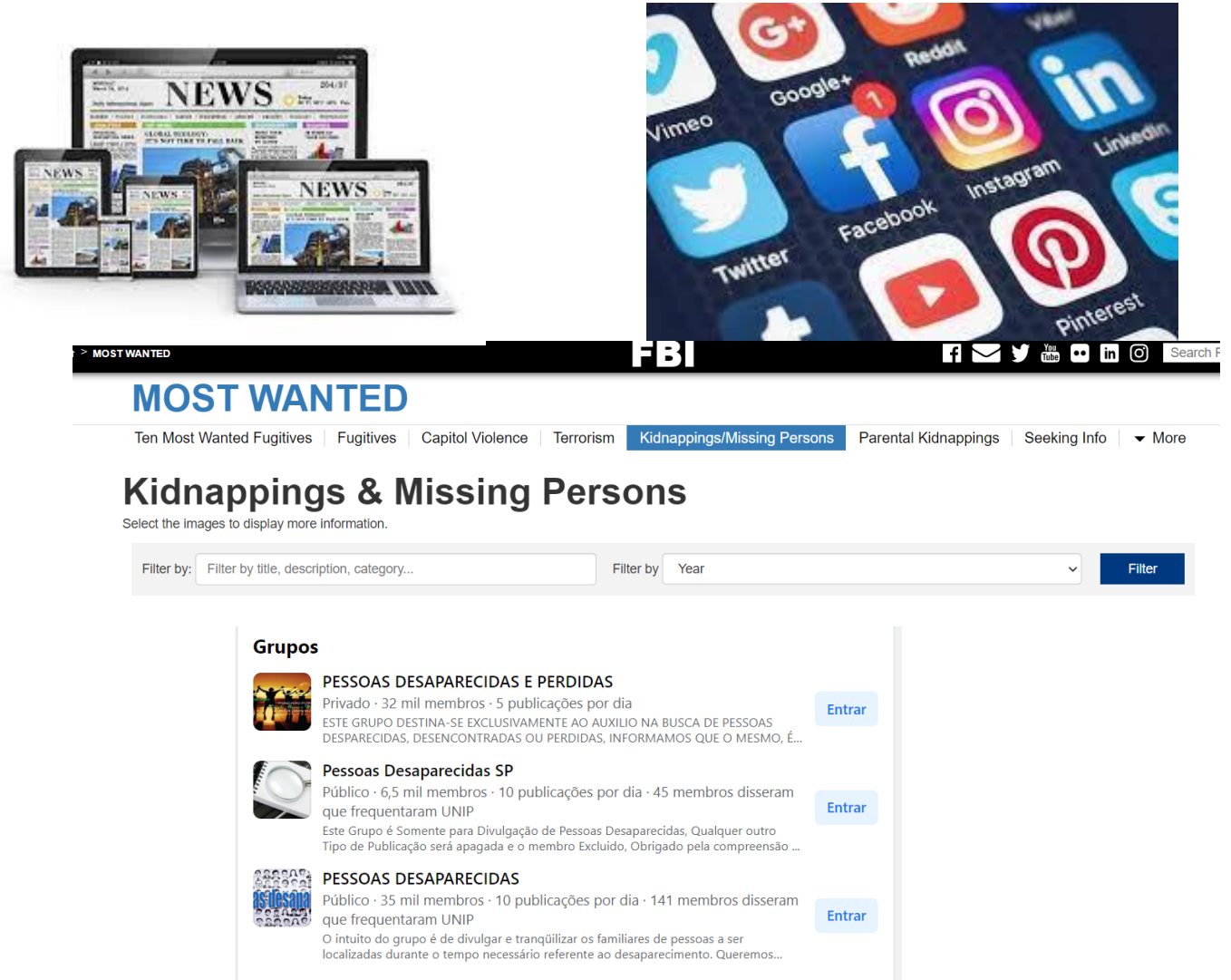
- Jeffrey's Image Viewer
- ExifTool by Phil Harvey
- Metapicz
- IrfanView
- Find Exif Data
- FotoForensics
- Forensically
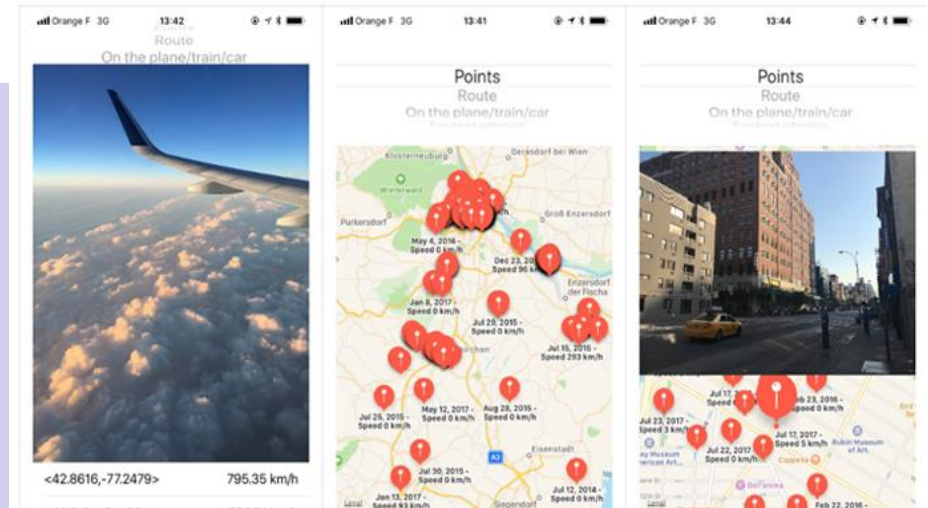
```
root@kali:~/Desktop/photos# exiftool -Copyright=KaliLinux DSCN0010.jpg
    1 image files updated
root@kali:~/Desktop/photos# exif DSCN0010.jpg
EXIF tags in 'DSCN0010.jpg' ('Intel' byte order):
--------------------+-----------------------------------
Tag                 |Value
--------------------+-----------------------------------
Image Description   |
Manufacturer        |NIKON
Model               |COOLPIX P6000
Orientation         |Top-left
X-Resolution        |300
Y-Resolution        |300
Resolution Unit     |Inch
Software            |Nikon Transfer 1.1 W
Date and Time       |2008:11:01 21:15:07
YCbCr Positioning   |Centered
Copyright           |KaliLinux (Photographer) - [None] (Editor)
Compression         |JPEG compression
X-Resolution        |72
Y-Resolution        |72
Resolution Unit     |Inch
Exposure Time       |1/75 sec.
F-Number            |f/5.9
Exposure Program    |Normal program
ISO Speed Ratings   |64
```

Useful techniques for investigating missing persons #3

- News is important for the study of a disappearance;

- Sites that list missing persons;

- Social media information helps a lot, especially friends, relatives and people who interact with you on a regular basis;

Important information for an investigation

Personal information:

- First name, last name, date of birth, personal documents, work or home address, personal phone number, email, social network profile, physical description, comments on social networks and interaction;
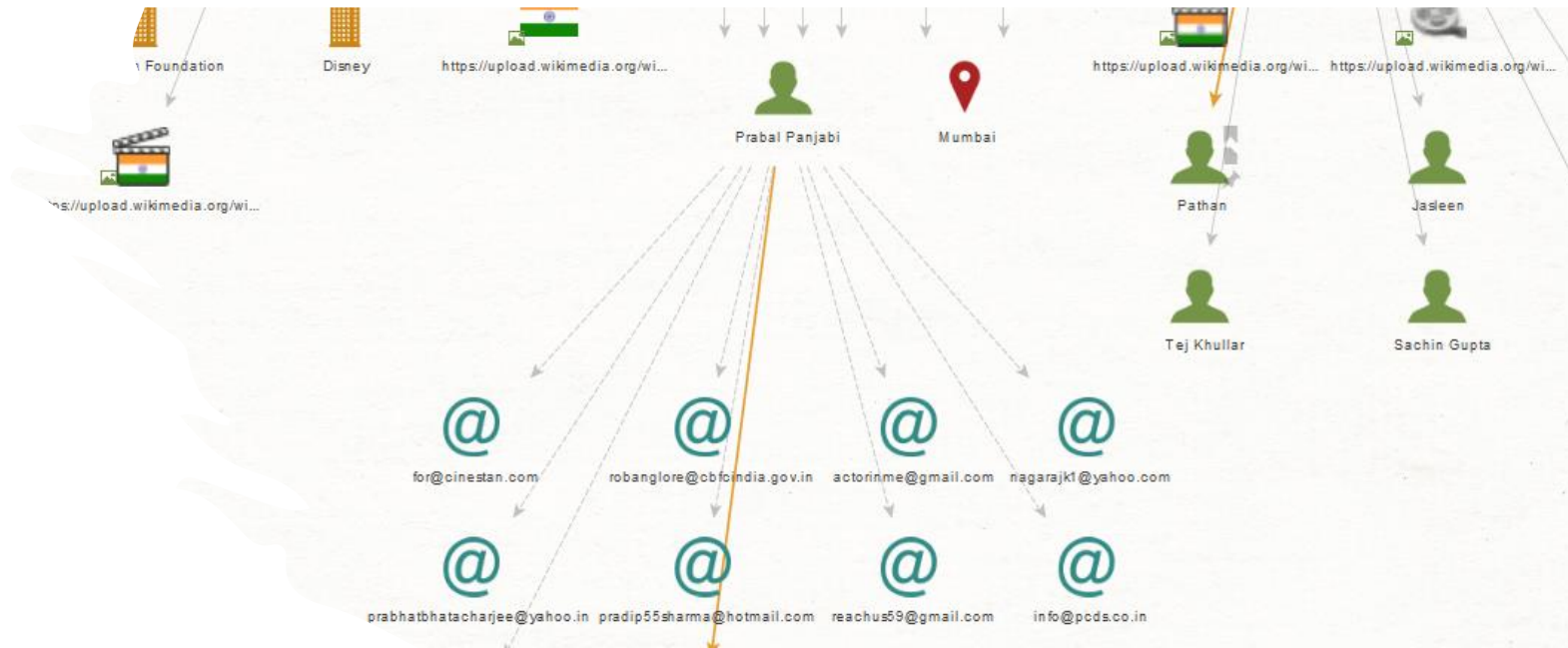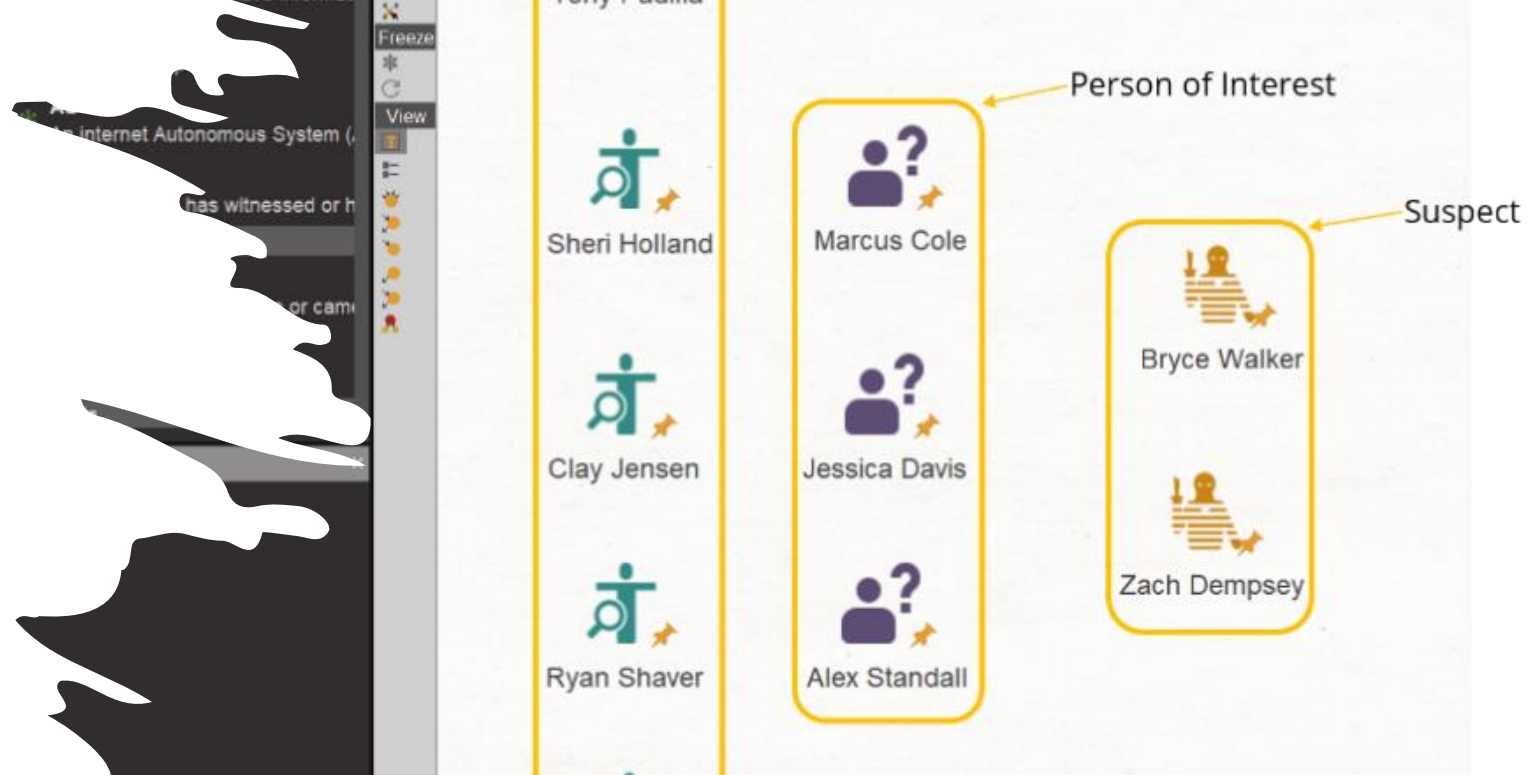
Family information:

- First name, last name, date of birth, personal documents, work or home address, personal telephone, email, social network profile;
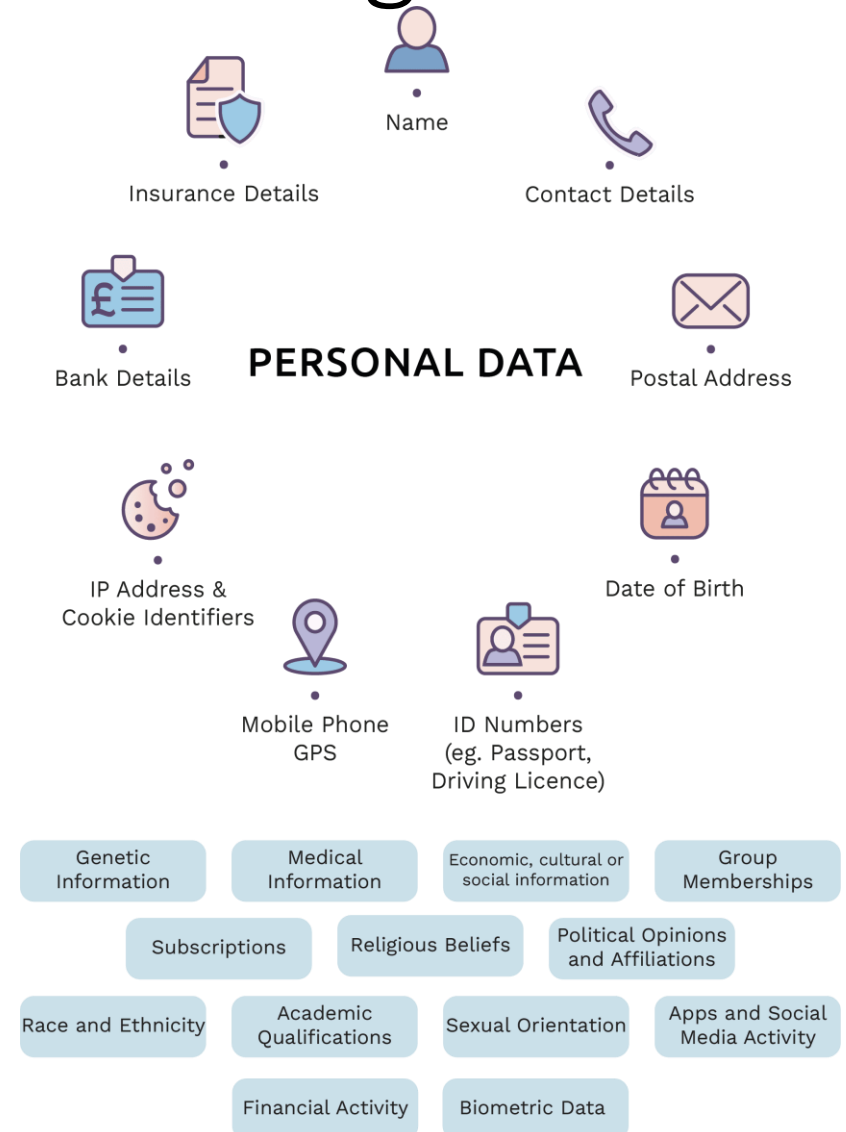
Conducting an investigation with Maltego

- An investigation using Maltego has three steps

- First, we map the full online presence of the target's name or alias, analyzing relevant sites and images.

- Second, we will try to find out any personal information, such as email addresses or phone numbers, from the target's online footprint.

- Finally, once we can confirm the identification of the target, we will move to advanced databases of persons of interest to obtain more specific identity intelligence.

Tools

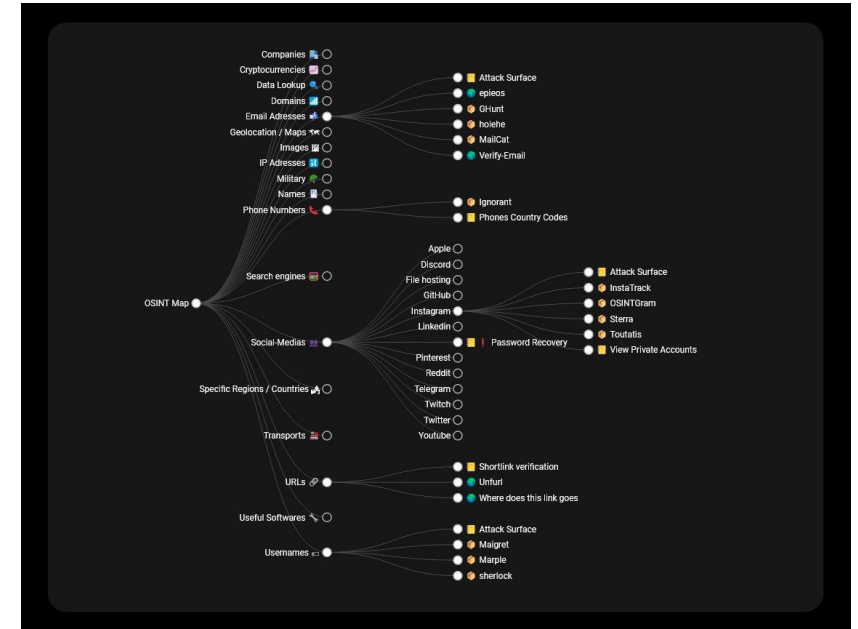# Thanks!!