HHNBO 29TH NOVEMBER 2018

OSINT FOR JOURNALISTS

Presented by: Peter Numi

#! WHO AM I

PETER NUMI

Security is my Thing

@th3_gr0ot

| MALWARE ANALYSIS |

| REVERSE ENGINEERING |

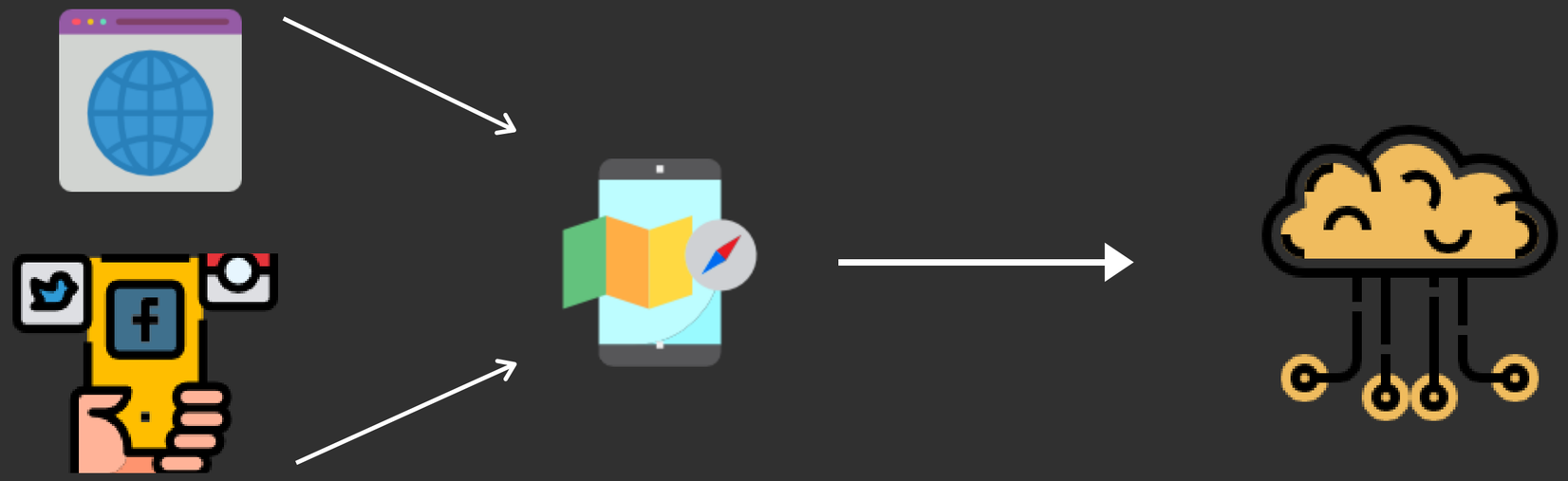
| OPEN SOURCE INTELLIGENCE | HARDWARE |

| OFFENSIVE SECURITY |

th33gr0ot.tk

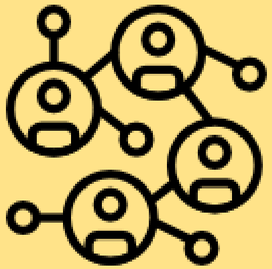
What Is Open Source INTelligence (OSINT)?

-THE USE OF PUBLICLY AVAILABLE DATA IN AN INTELLIGENCE CONTEXT.



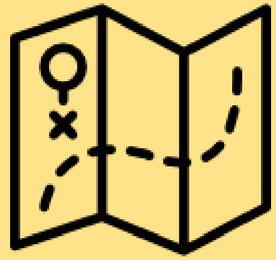
SOURCES OF INFORMATION

The Internet



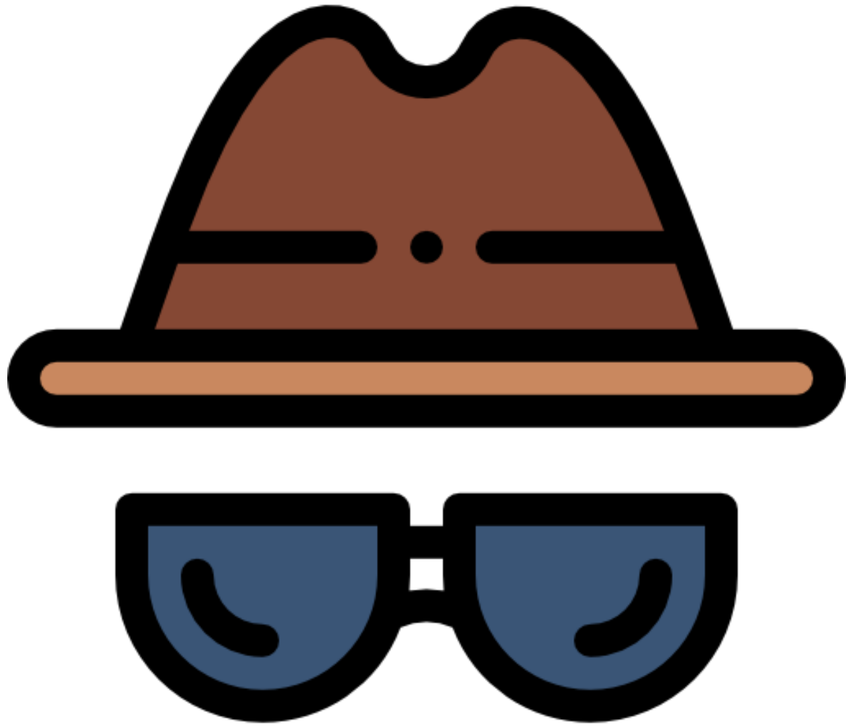
Social Media

Public Records



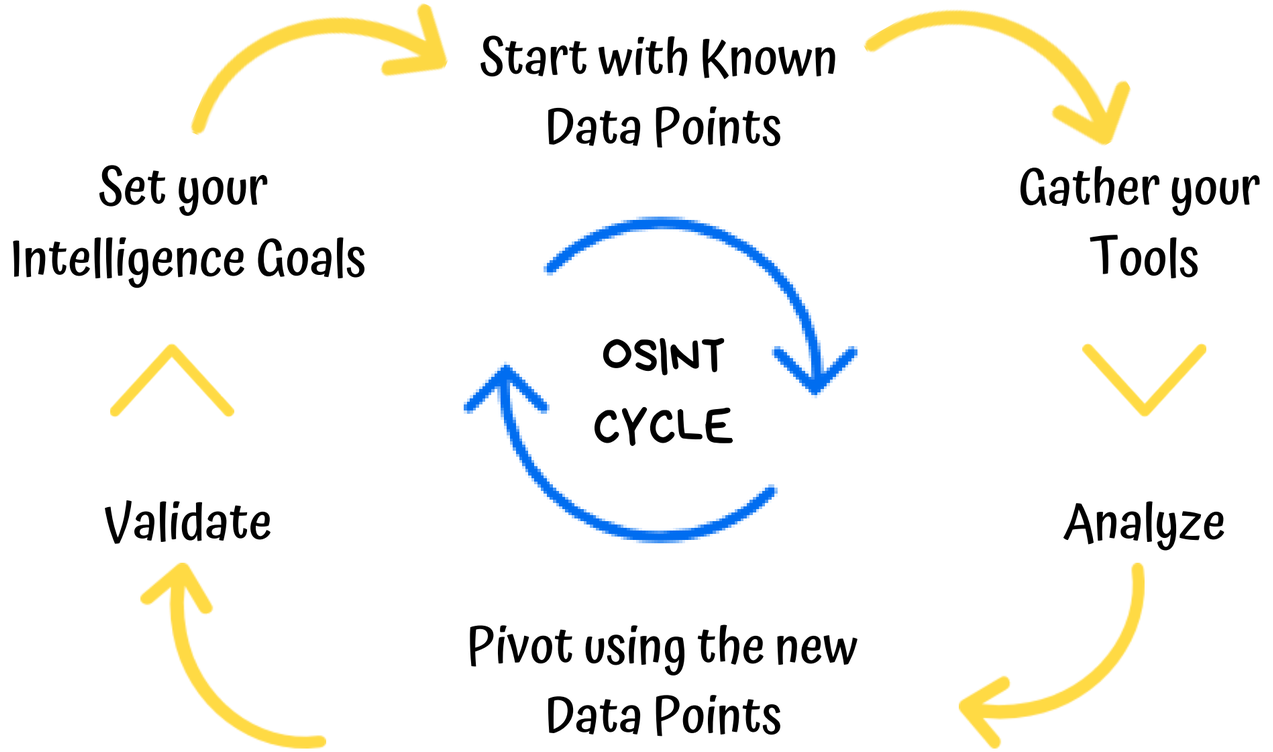
Geospatial Information

Traditional Mass Media



OSINT METHODOLOGY

OSINT is all about following the footprint's, here is a methodology by Josh Huff an OSINT Creeper.



GOOD OPerationSECurity

Good OPSEC is all about maintaining privacy.
You can maintain good opsec by:

Separating your social life from your work life.

THIS BASICALLY MEANS MAKING SURE THAT NOT TOO MUCH OF YOUR INFORMATION ISN'T PUBLIC AND USE OF SECURE COMMUNICATION CHANNELS.

TOOLS

Twitter Deck

Intel Techniques by Michael Bazzel

Firefox Screenshots Beta

Take, save, and share screenshots without leaving Firefox.

OSINT FRAMEWORK

https://osintframework.com

INTERNET ARCHIVE WayBackMachine

Tails theamnesicincognitolivesystem

Tutanota®

Encrypted, Open Source Email Service

DEMO

SHALL WE PLAY A GAME

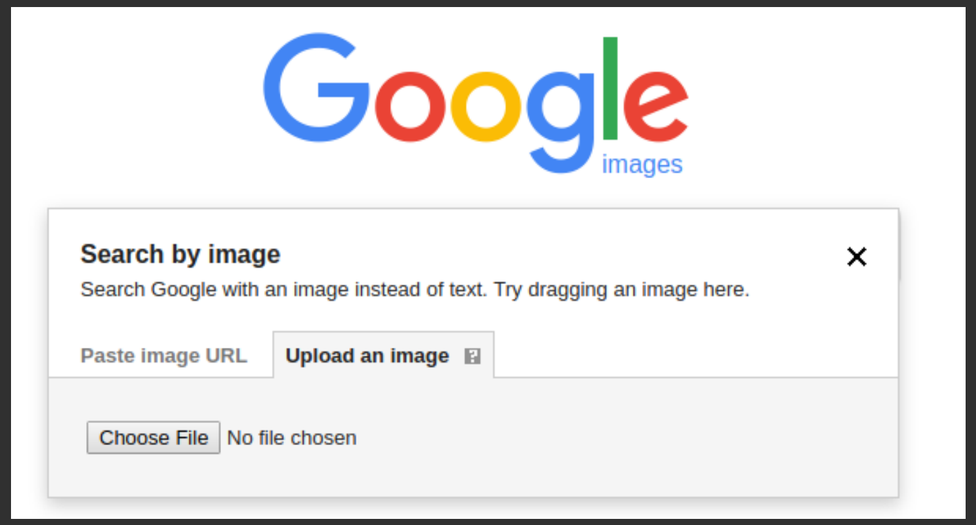
Disclaimer: This is a Fictional Story, it is not true and everything included in this DEMO is for learning purposes only.

Story Line:

There lived a young orphan who was a boy and his name was groot. Groot lived in Lebanon and this year he was moving to a new children's home. When he went to his new home there were rumors that there was a boy who left the children's home and went online to create an al-shabaab Facebook profile with the home's image as his profile picture which is diminishing the home reputation. Let's help groot find this boy and his whereabouts.

REVERSE IMAGE SEARCH

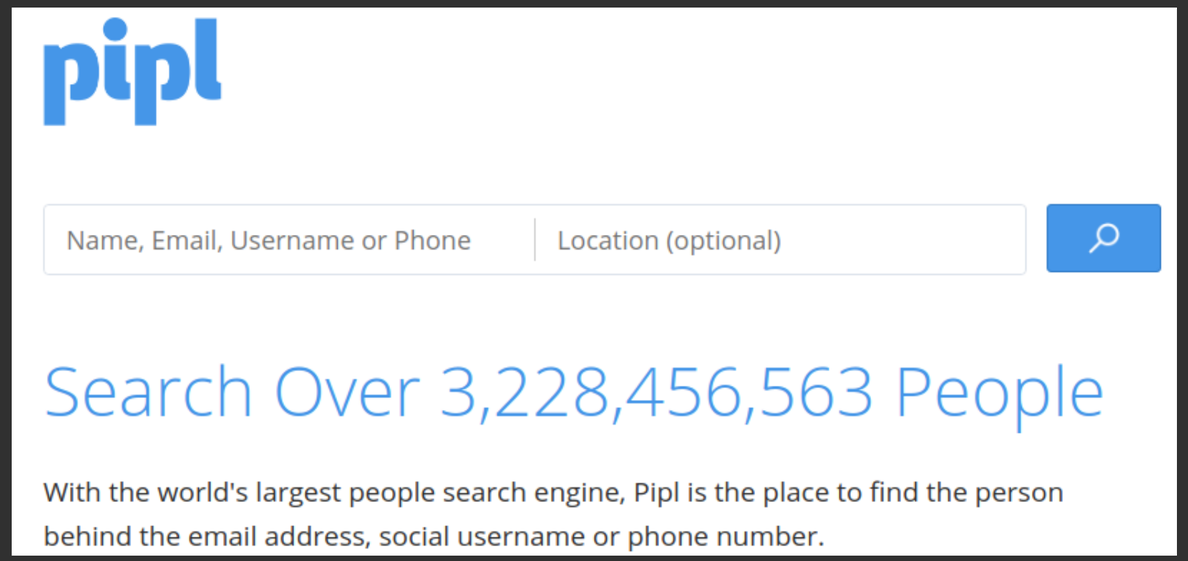
Objective: Finding the young boy using the clues provided.



PROVIDED CLUE:

PEOPLE SEARCH

Objective: Finding a needle in a haystack, his location.



PROVIDED CLUE:

On Social Media he uses the name: Alshabab Alwatani

GEOLOCATION

Objective: Location Triangulation.

PROVIDED CLUE:

- He loves Sea Food
- Currently at the Da Vinci Science Center

WEB ARCHIVE

Objective: Locating the Father and Old website he owned.

PROVIDED CLUE:

- Father used be a CEO of a dairy product company and he loves to tweet alot.
- Website Link:

http://southseasfoods.com:80/

GOOGLE + PIVOTING

Objective: Identifying any relationships.

PROVIDED CLUE:

- Nammarico Corp

GOOGLE + PIVOTING

Objective: Pivoting using new Data Point

PROVIDED CLUE:

- @drinklavish

!! DONE !!

Objective: Finished, no proven data to validate.

LavishGrindENT

@LavishGrindENT

The Official Twitter of LavishGrind Entertainment Est.2016

Detroit, MI

PROVIDED CLUE:

- This being a Demo for Learning purposes their is no valid data to validate, but he is our Objective

>> JAY OHSO

REFERENCES

AMAZING RESOURCES TO LOOK INTO

Beyond finding the right tools, what's Strick's advice for other journalists or hobbyists who want to conduct their own digital investigations?

"Do something small, like finding your neighbor's cat ... think like Carrie Mathison from 'Homeland,'" he said. "That's the cool thing about this — anyone can jump into this community."

1. OSINT TECHNIQUES :https://www.osinttechniques.com/osint-tools.html
2. BBC OSINT Report by Poynter on how they did it: https://www.poynter.org/news/how-bbc-verified-video-grisly-murder-cameroon-step-step
3. Josh Huff, What I learned by being an OSINT Creeper: ttps://www.youtube.com/watch?v=6kBOCnOlwqI&t=128s

Thank you