PESU ISFCR

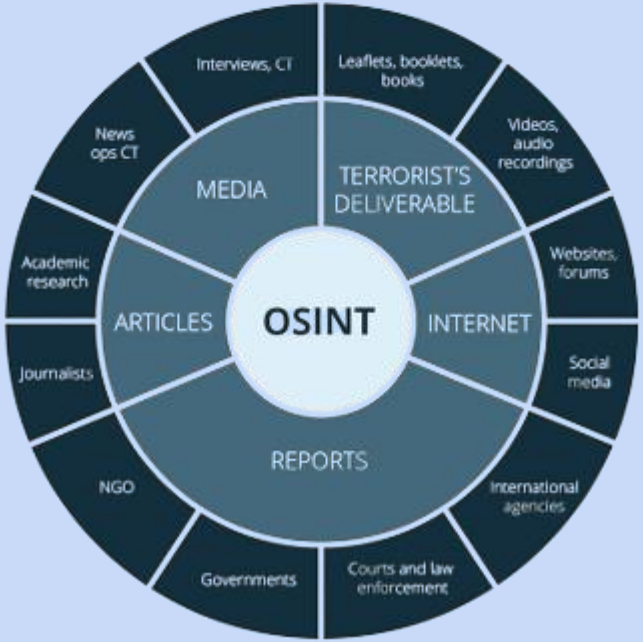
OSINT (Open Source Intelligence)

Hacktober 2021

OSINT is publicly available information on

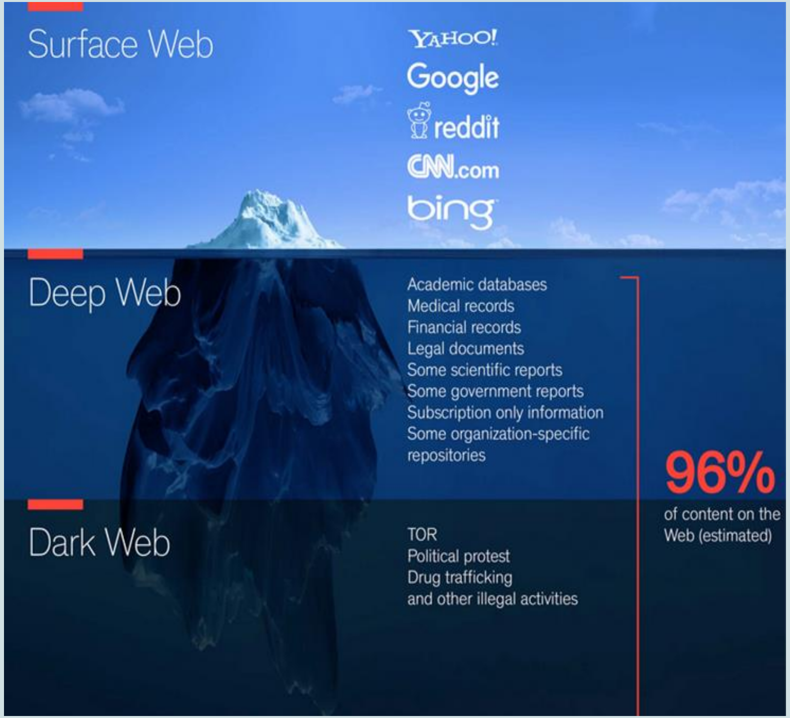
- People,
- Businesses,
- Networks,
- Domains etc

NOTE: Data/information Gathered may or may not be "free"



SOURCES

- Surface Web:
  - Google Search/Dorks
  - Public Records
  - Information gathering sites
  - Shodan
  - Social Media etc
- Deep Web:
  - Private forums/Networks
  - Hidden Wiki
  - Medical Records
  - Military Data etc
- Dark Web:
  - Tor
  - SecureDrop
  - ZeroBin etc



Why OSINT?

- OSINT is important for the Government, Investigators, Corporate Agencies ,Law Enforcement Agencies and even Penetration Testers.

- A practical example: Scambaiting

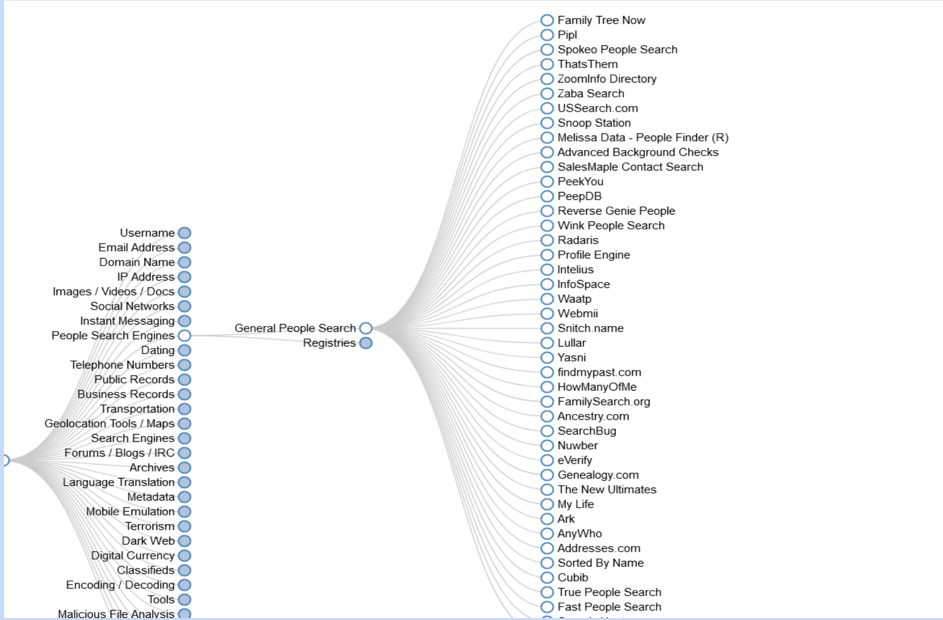
OSINT Methodology

1. Requirement definition
2. Data gathering
3. Analysis of data
4. Form Relationships with data
5. Validation of assumptions
6. Report generation

OSINT Framework

It is a combination of various OSINT tools for recon and digital footprinting.

[DEMO]

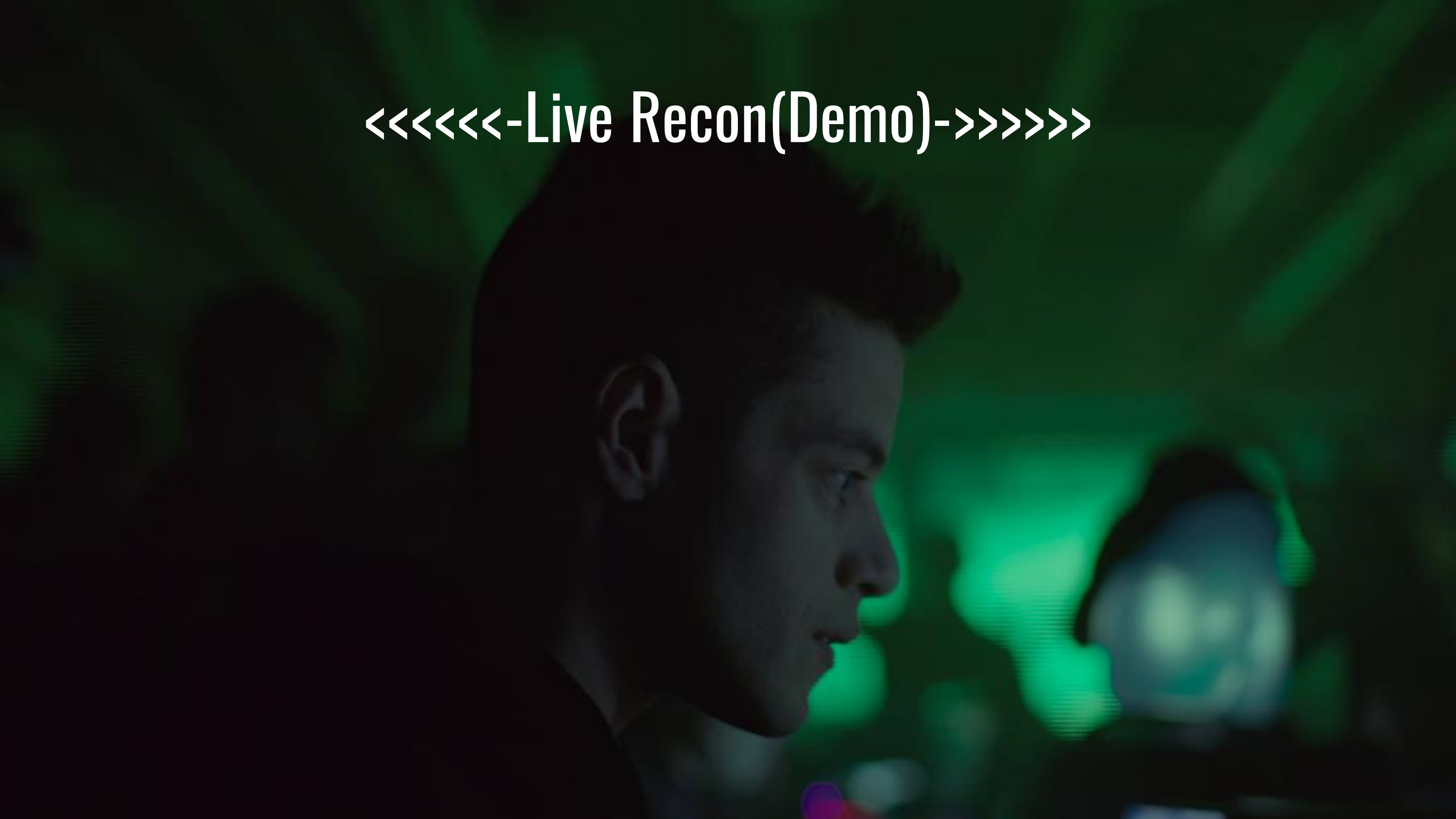


OSINT from the CTF Perspective

Tools/Interesting links:

- This is the collection of tools which I use while playing CTFs(several others as well): https://github.com/echobash/commonErrorsTricksAndHotfixes/tree/master/CTF/osint
- https://www.radarbox.com [Flight Data]
- http://www.cell2gps.com/ [Cell Tower Locator]
- https://pimeyes.com/ [Facial Reconnaissance Engine]
- https://www.shodan.io/ [IoT Search Engine] and many more…

<<<<<<-Live Recon(Demo)->>>>>>



Thank you!
See you soon!