GEOINT

Tracking down locations in digital investigations

@AtomicNicos

Open Source INTelligence / Recon

Relies on publicly available data:

Social media accounts

Phonebooks

Documents

…

Usually less reliant on:

Interaction (HUMINT)

Communications technologies (SIGINT)

Equipment Analysis (TECHINT)

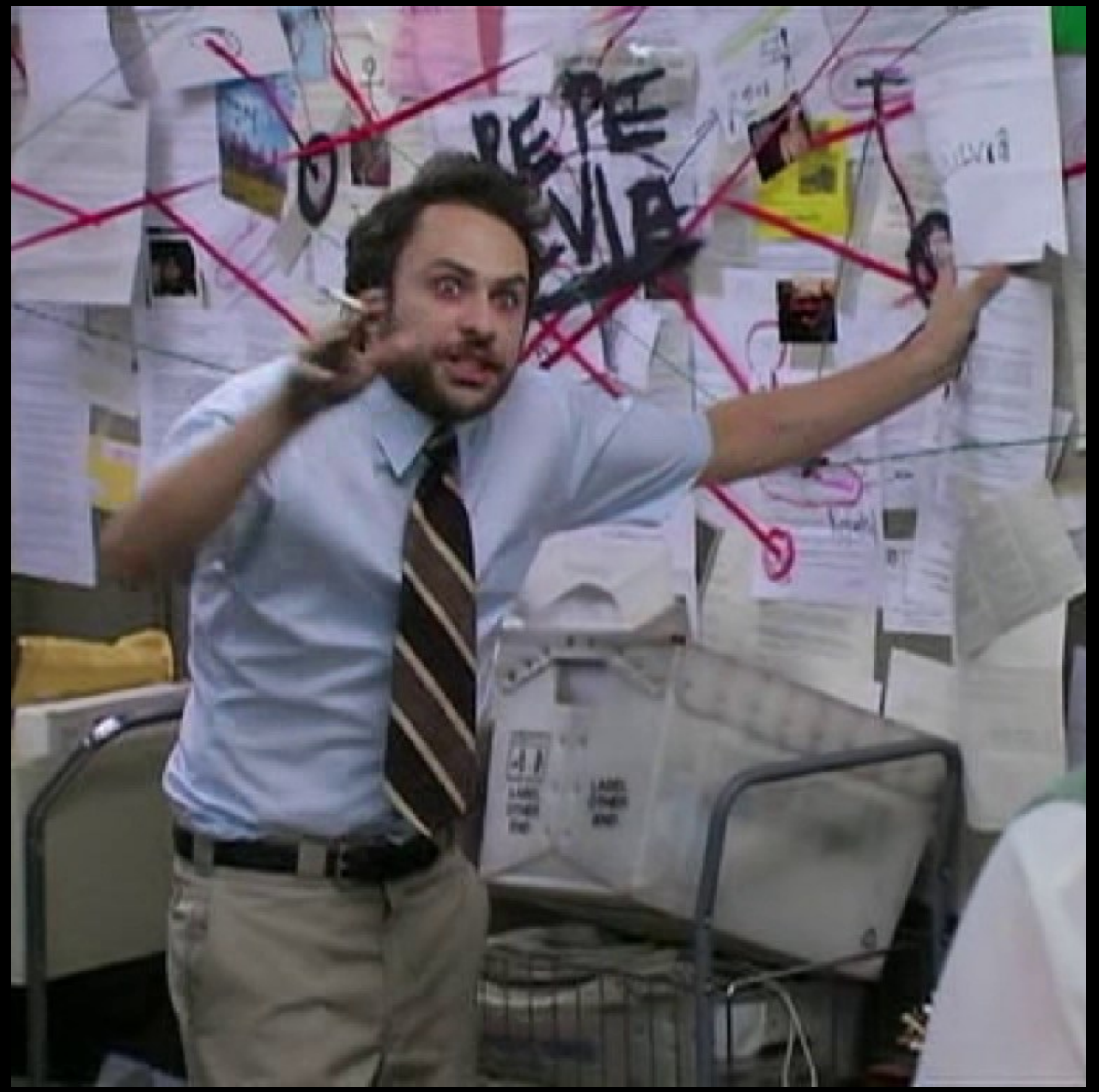
…

OSINT Steps

DEFINE REQUIREMENTS → RETRIEVE DATA → ANALYZE → PIVOT → REPORT

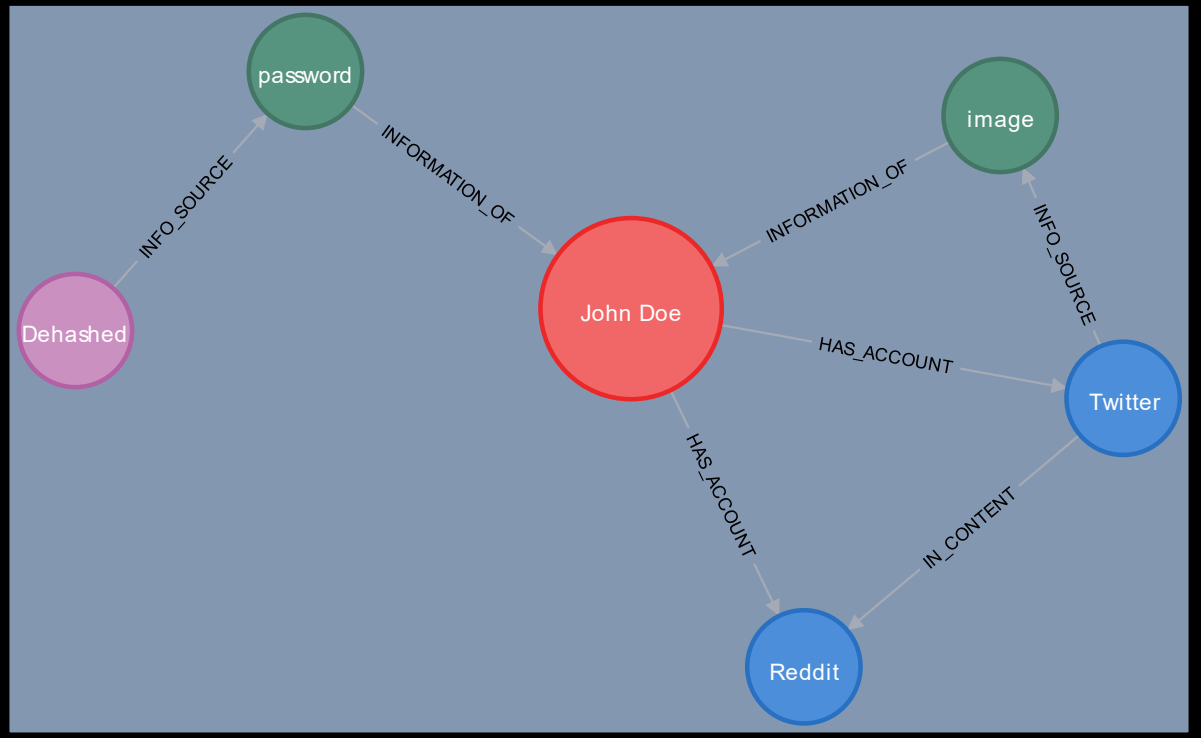
Pivoting

Looking less like this



Pivoting ?

- Get datapoints from a previously collected datapoint
- Use it to grow the dataset



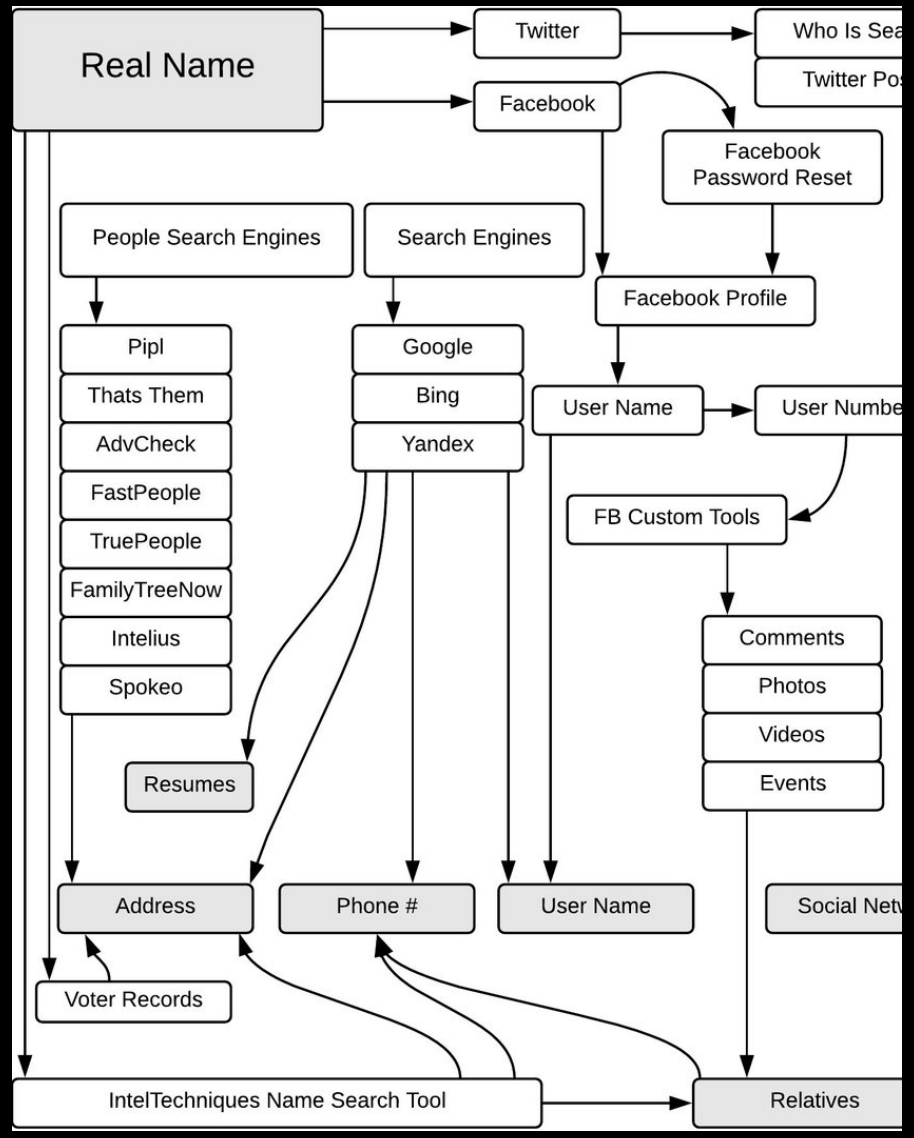
First pivots

- Find social media ! (Google dorking, …)
  - Result: Relations profile (family, friends, …)
- Find pictures
  - Physical profile (body modifications, tattoos, haircut, …)
  - **Locations**

Advanced pivots

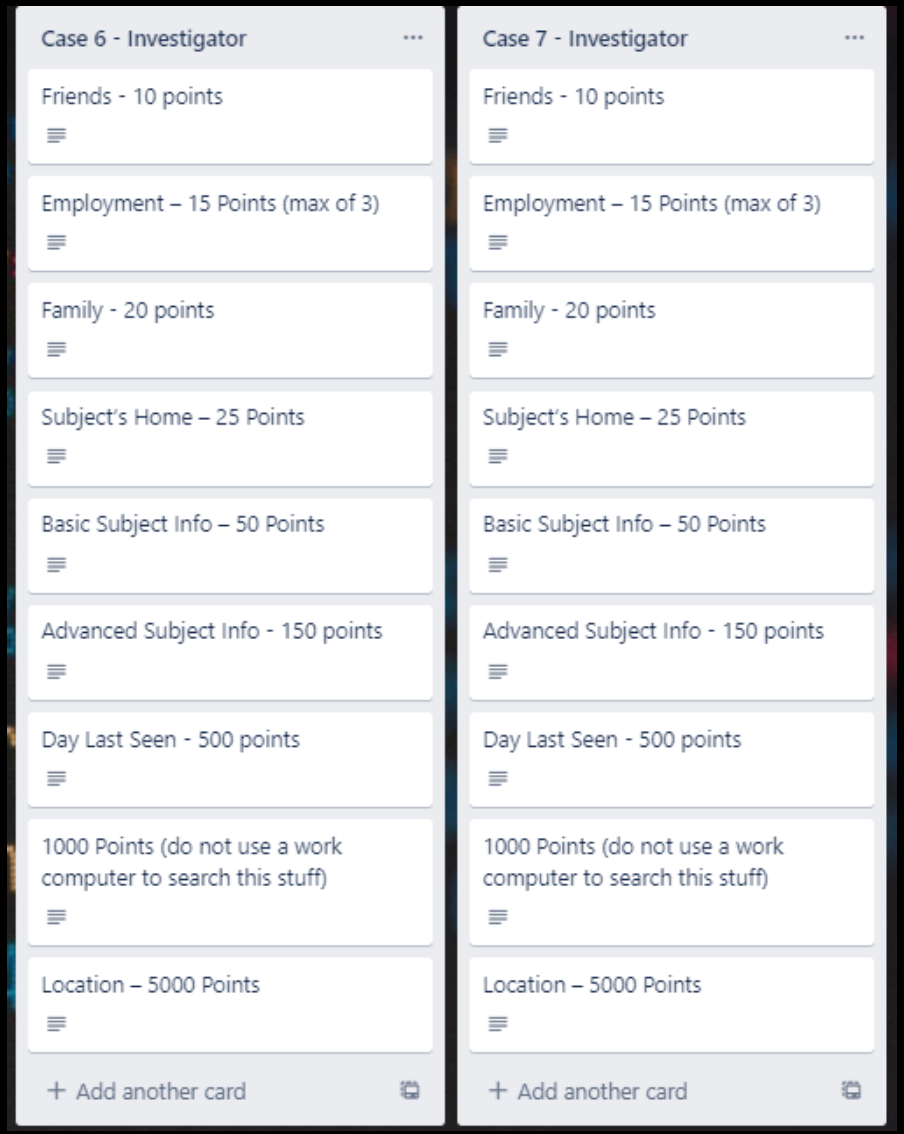
- Name changes (→ Aliases, Records, …)
- Yellow / White pages (→ **Addresses**, Assets, …)
- Dehashed, RaidForums (→ Credential Leakage, …)
- Criminal Records (→ Affiliations, …)

Credit: Petro Cherkasets



Tracking steps

- Finding data once is cool, having to find it again is a waste of time.
- Store information type, a short description, URL's, snapshots.
- ⚠ Also note how you got there !



How can I infer?

How can I infer?

Demonstration

https://twitter.com/juan_spinel/status/1396151405677879296

Availability

Work licensed under Creative Commons : CC-BY-SA (legalcode)

Open License

Under the following terms:

Attribution — You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

ShareAlike — If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original.

No additional restrictions — You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits.

AMA

Discord : @AtomicNicos#1404
Twitter : @AtomicNicos