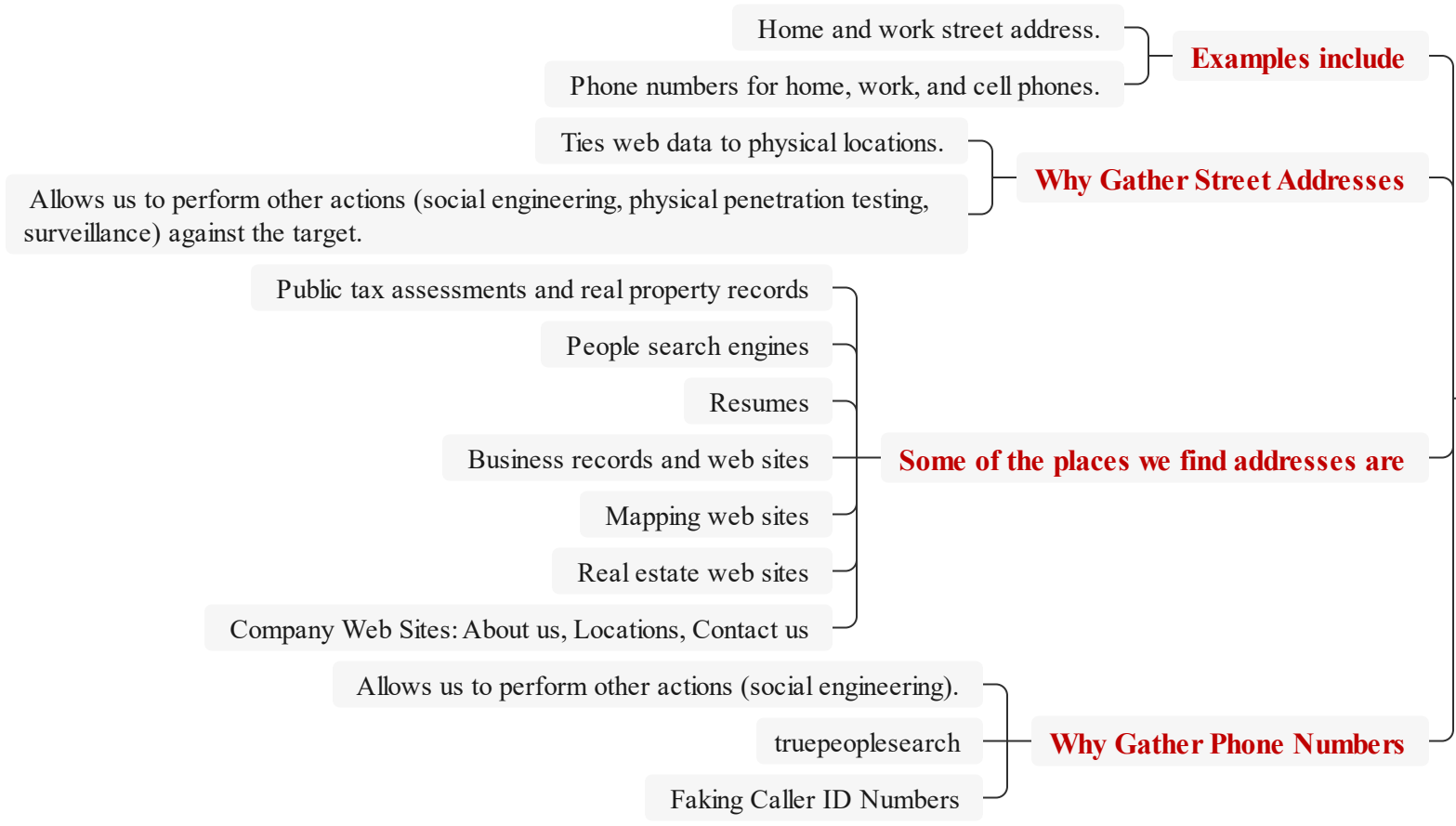


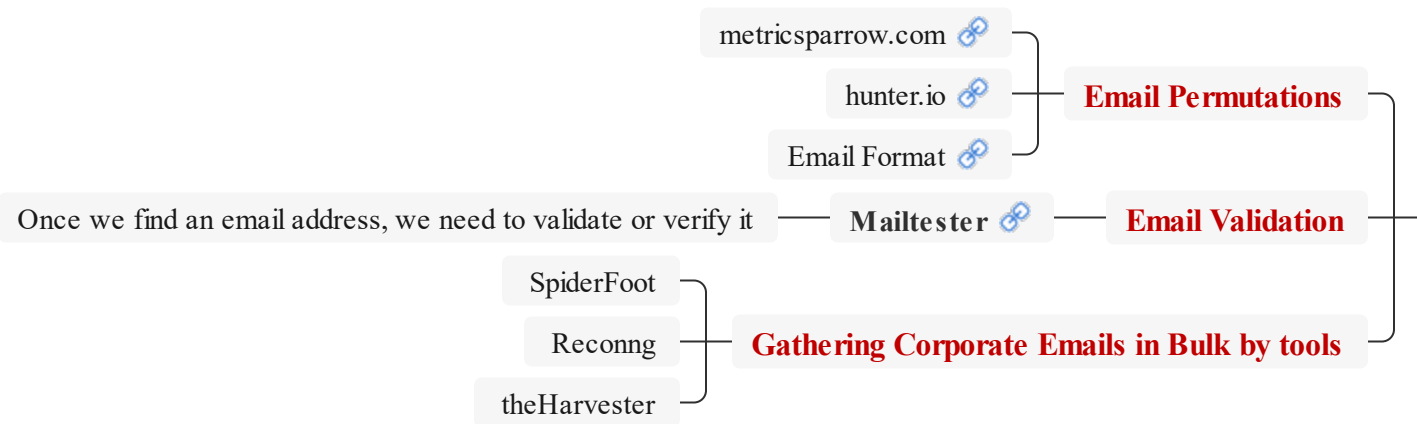
LinkedIn: @muhammed-dardir

Day 2 Gathering, Searching, and Analyzing OSINT

5. Basic Data: Addresses and Phone Numbers



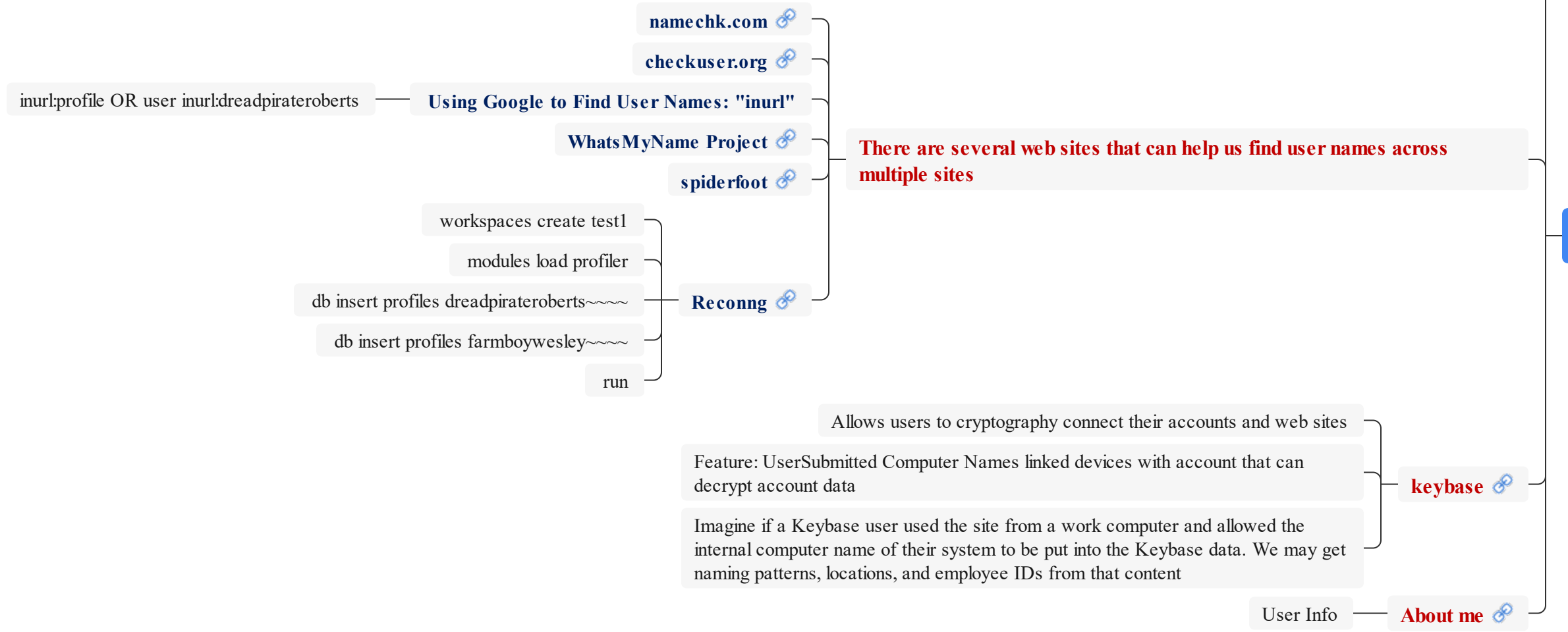
6. Basic Data: Email Addresses



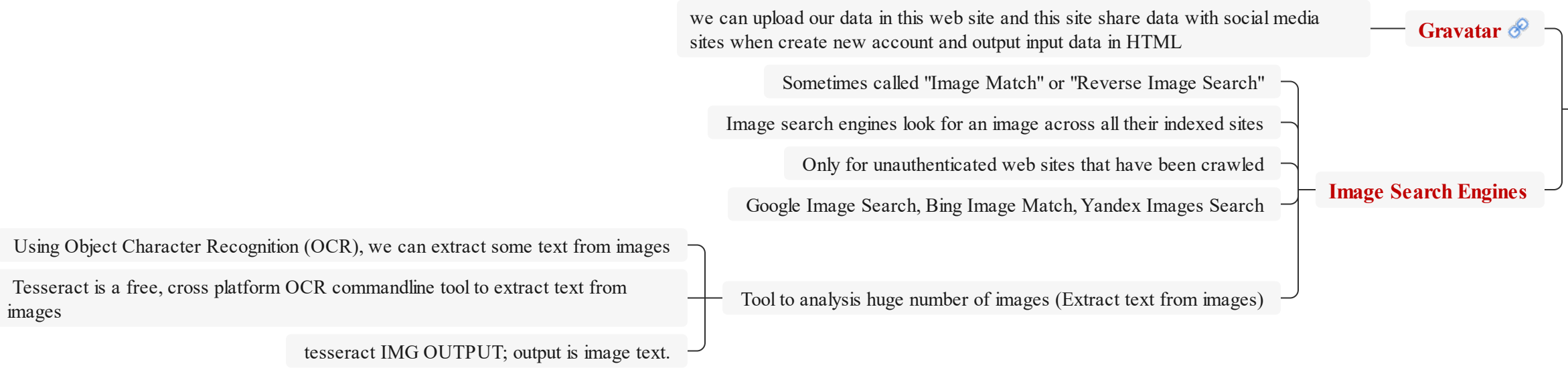
Process

1. Find all the user names your target(s) may use
2. Find all the web sites where those user names are valid
3. Examine which user accounts are for your target(s)
4. Retrieve data about target(s) from user profiles
5. Examine relationships
6. Examine activities
7. Pivot

7. User Names



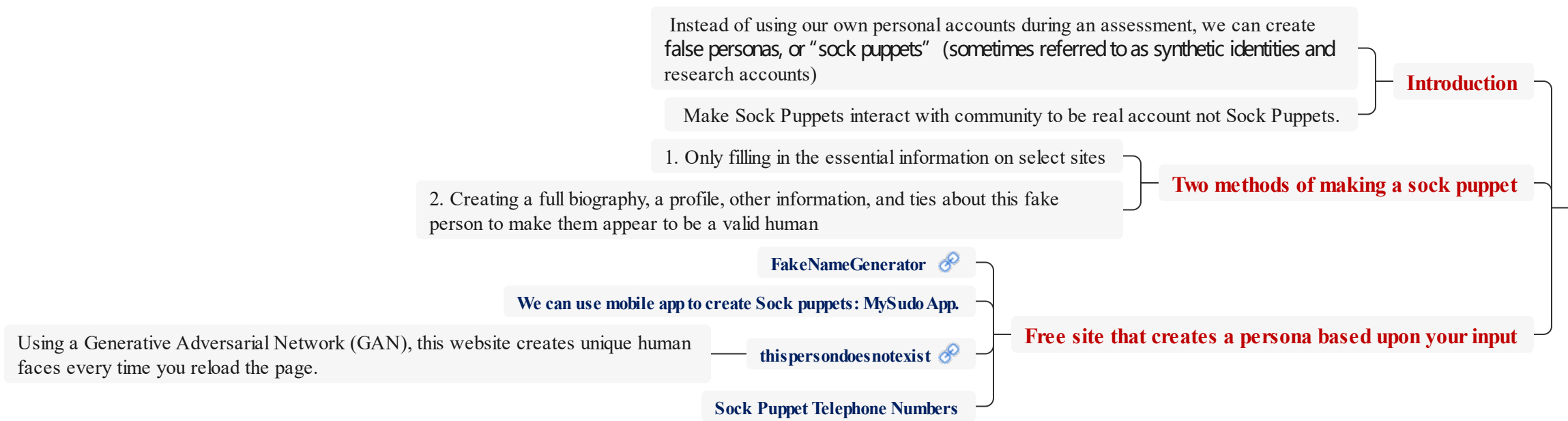
8. Avatars and Reverse Image Searches



9. Additional Public Data

- There are web sites that allow us to search for wedding registries
- LinkedIn Profile Confirmation and Marriage License
- Obituaries and Death Notices [Legacy.com for Death Notices]

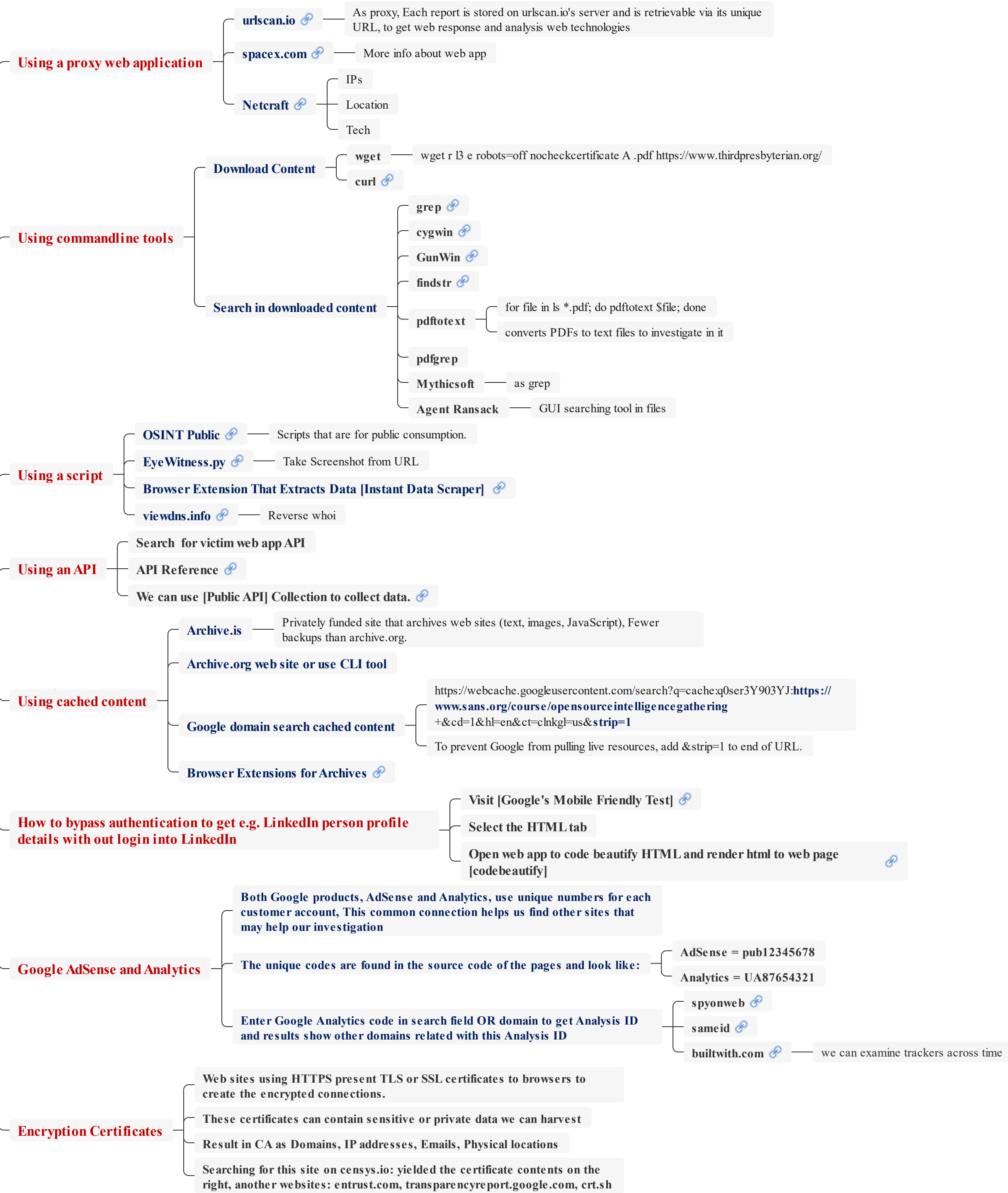
10. Creating Sock Puppets



1. Data Analysis Challenges

- Potential reasons for inaccurate data**
 - Active measures by your target (Planting a false trail): Here we have a target that has intentionally placed false data
 - Unintentionally incorrect data (OCR, Siri, typos): Humans enter data not accurate.
 - Old data that wasn't updated (whois): The whois system is an excellent example of this class of false data.
 - Similar target's data (Multiple people, same names): Your target's name is very common for the region you are searching.
 - Human nature (Bragging, appearing to be someone they are not – think online dating profiles): people who share/post data wrong in social network
- Correlation Does Not Imply Causality**
 - Correlation: means that a relationship exists between two or more things.
 - Causality: is different. With causality, one thing makes something else happen.
- Sound Analysis**
- Free PDF on Analytical Thinking** — Psychology_of_Intelligence_Analysis.pdf

2. Harvesting Web Data



3. File Metadata Analysis

- Exiftool**
 - CLI or GUI
 - Extract GPS — exiftool c %+.7f GPSPosition *.jpg
And use output in [Google Maps]
- thexifer** — Web APP WARNING: Sharing files
- verexif: Web APP** — WARNING: this web app Sharing files
- FOCA (Fingerprinting Organizations with Collected Archives)** — FOCA is a tool that has been well known for metadata analysis of files.

4. OSINT Frameworks

- OSINT**
 - OSINT Project
 - OSINT Source Code
- Technisette**
- OSINT Team Links**
- Onstrat website**
- Reuser web site**
- (OSINT) Recherche training**
- Terrorism & Radicalisation Research Dashboard** — Looking for international terrorists and the systems and tools they use?
- OSINT analysts that need to venture into the world of dating and sx sites**
- Bellingcat** — Bellingcat maintains a Google document with well categorized links for international OSINT
- D3 by Observable** — To Build your own Visualization