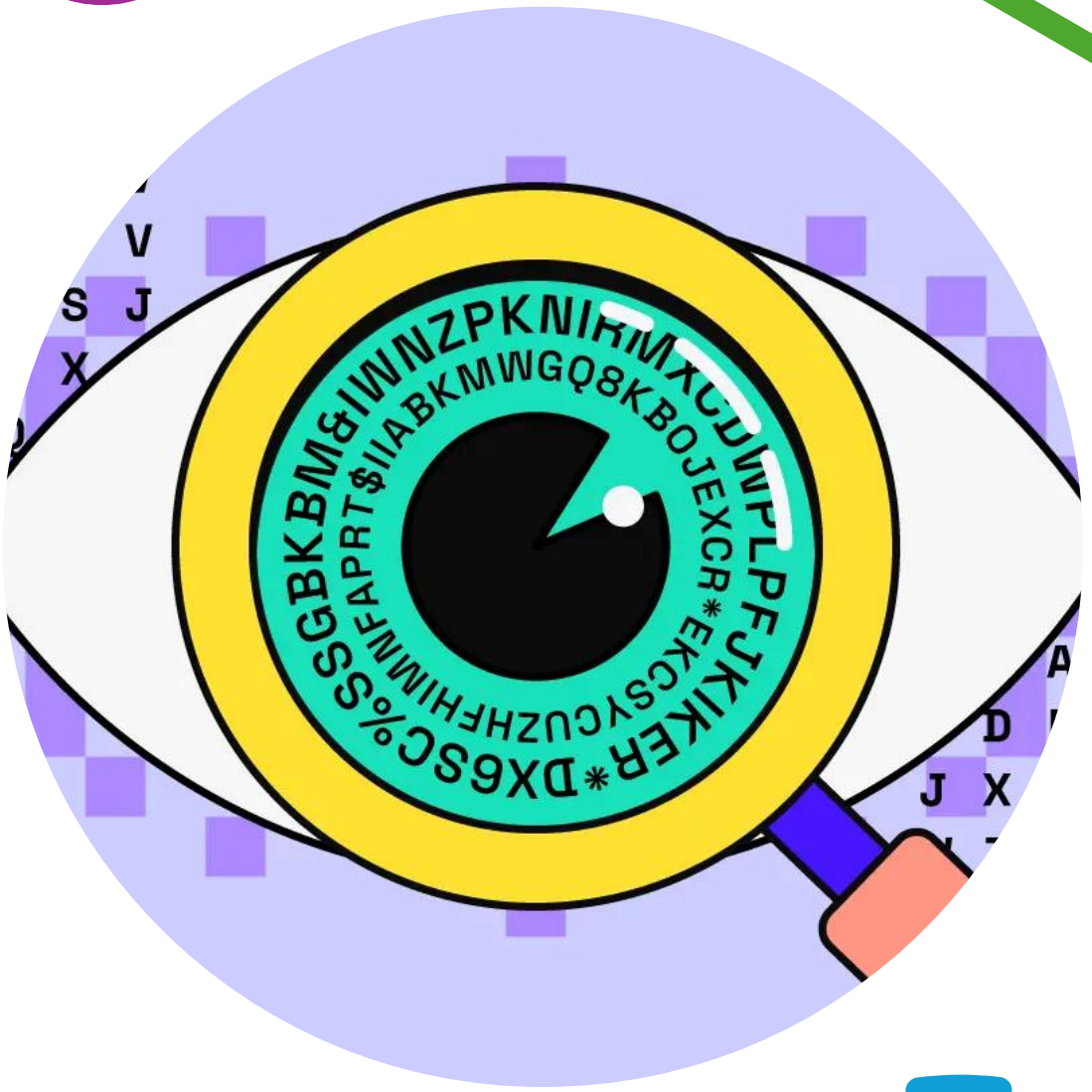


Open-Source Intelligence (OSINT)

Outlines

- What is OSINT?
- Data, information, and intelligence
- Where/Why is OSINT used?
- OSINT Process
- OSINT Frameworks

Nauman Munir

What is OSINT?

OSINT (Open-Source Intelligence) is the process of gathering and analyzing publicly available data which can be found either online or offline.

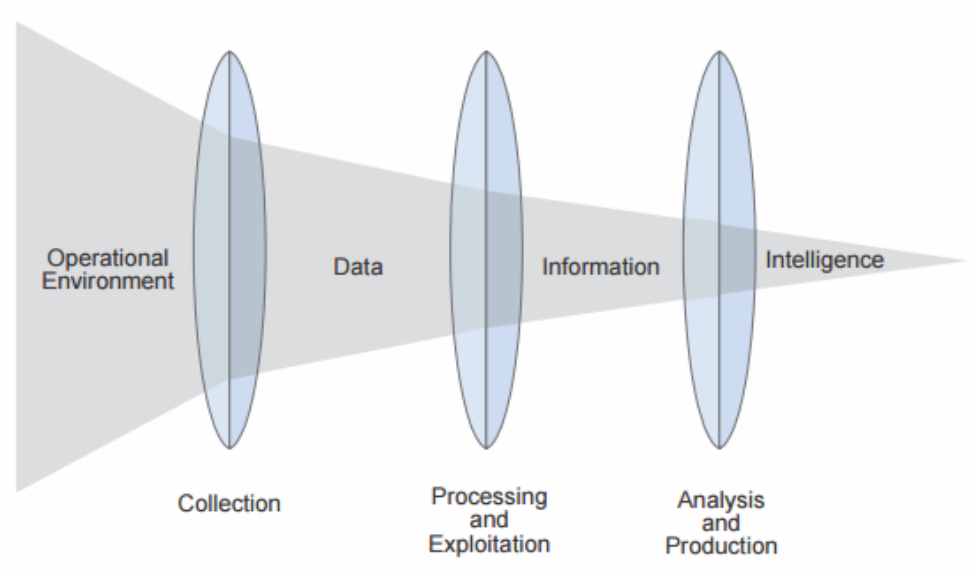
Some Examples:

- Traditional Media (newspapers, books, magazines, television and radio)
- Academic Sources (papers and conferences)
- Geospatial Information (maps)
- internet (online publications, video sharing sites, blogs, forums and social media websites)

Data, information, and intelligence

OSD (Open-Source Data)
Raw data from public sources
Example: Social media posts, news articles

OSIF (Open-Source Information)
Processed and contextualized data
Example: Compiled reports, summaries



OSINT (Open-Source Intelligence)
Analyzed information with actionable insights
Example: Threat assessments, intelligence reports

Where/Why OSINT is used?

Governments
Example: National security, policy making

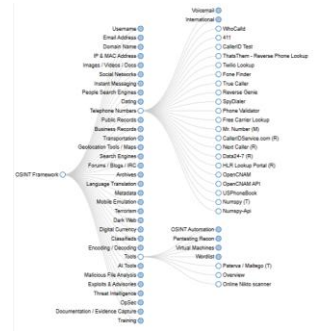
Law Enforcement Agencies
Example: Criminal investigations, Tracking criminal Networks

Business Corporations
Example: Market research, competitor analysis

Cybersecurity
Example: Detecting phishing campaigns, Identifying fake accounts, exposed databases

OSINT in Cybersecurity

Osintframwork.com
It is a collection of free online tools for research.



Shodan.io
Search engine for internet-connected devices

Google Dorking
Advanced search for hidden information.

Reverse Image Search (RIS)
RIS allows you to input an image and find its source.

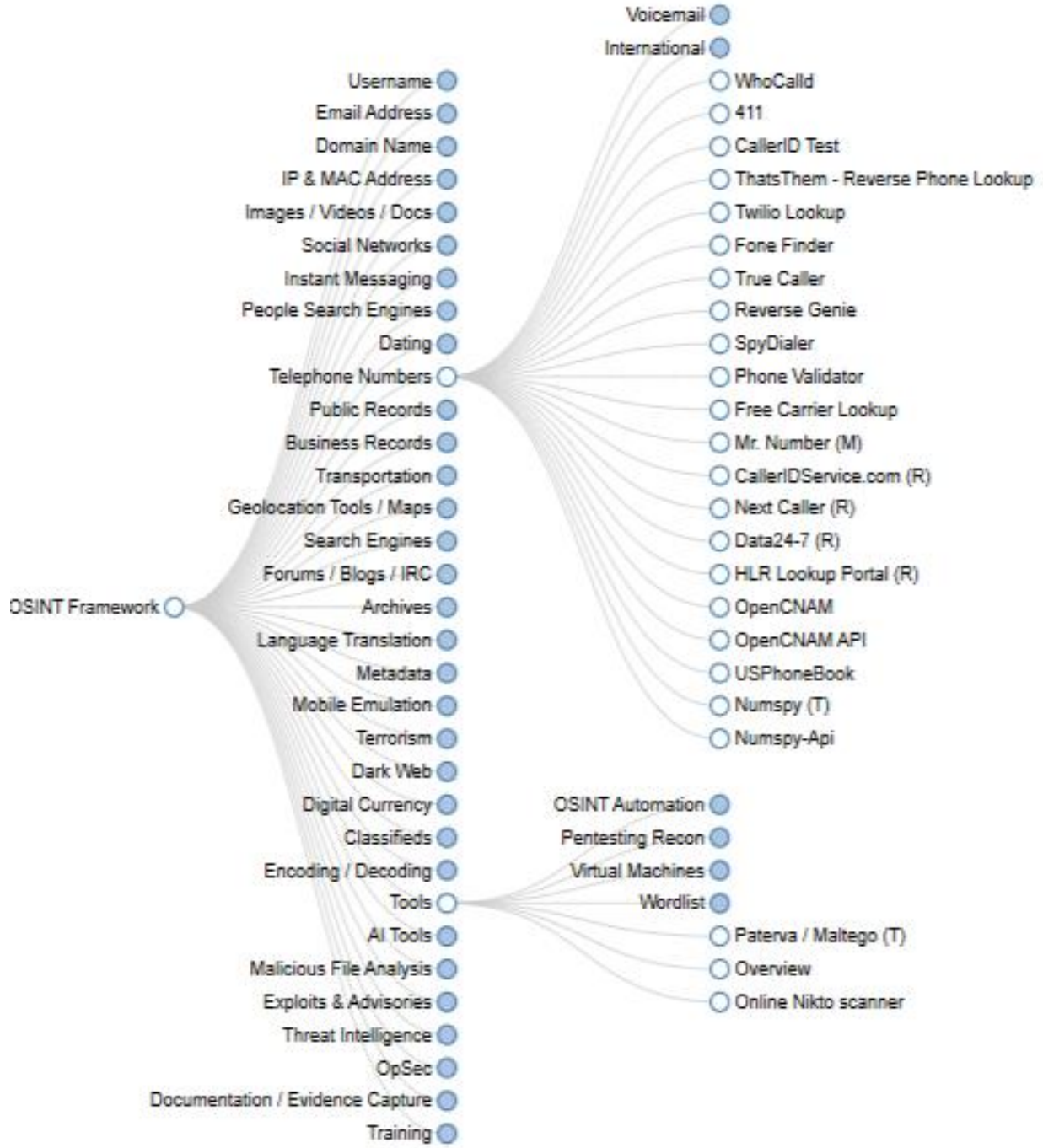
OSINT Framework

Osintframework.com

OSINT Framework is an organized collection of links, tools, and websites that help people gather information from publicly available sources.

Examples:

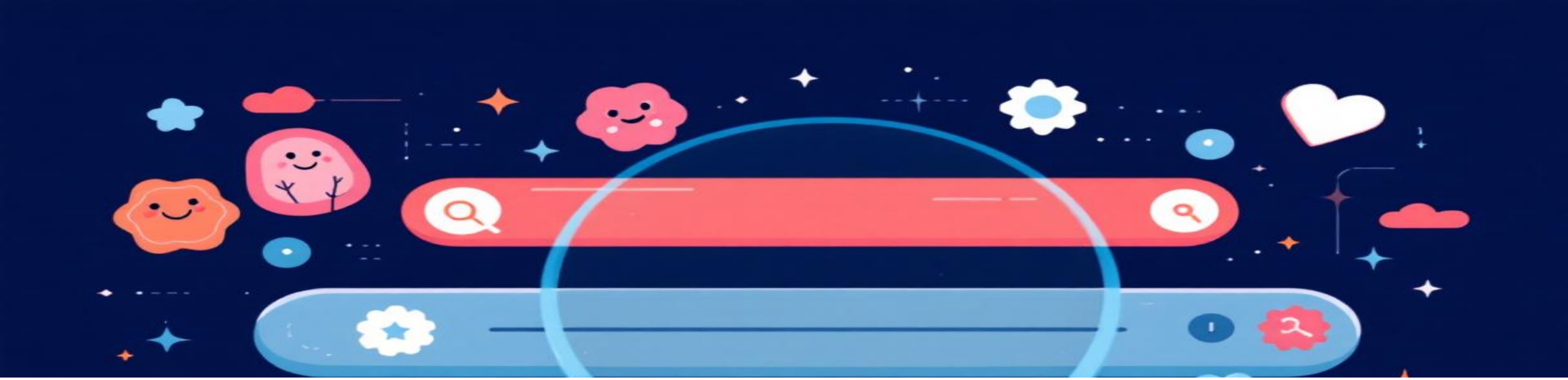
1. Find hidden data in photos. (EXIF metadata)
2. View deleted tweets or posts. (Archiving)
3. See where a phone number is registered. (Phone lookups)
4. Find other accounts with the same username. (Username enumeration)



Shodan is a search engine that scans the internet and shows devices that are connected online — like cameras, routers, servers, and IoT devices.

Queries:

- **Allows an attacker to steal private data (like keys and passwords):** vuln:ms17-010
- **Smart Doorbells & Cams: product:** "Hikvision IP Camera" country:AE
- **Devices running Windows Remote Desktop:** has_screenshot:true country:AE



Google Dorking

Google Dorking, or advanced searching, uses special operators to filter results, finding information you could never access with a simple search term.

site:targetwebsite.com
Limits search results to a specific website. Excellent for finding hidden pages or old press releases.

filetype:pdf OR doc
Searches for specific file types, often revealing publicly posted policy documents or sensitive reports.

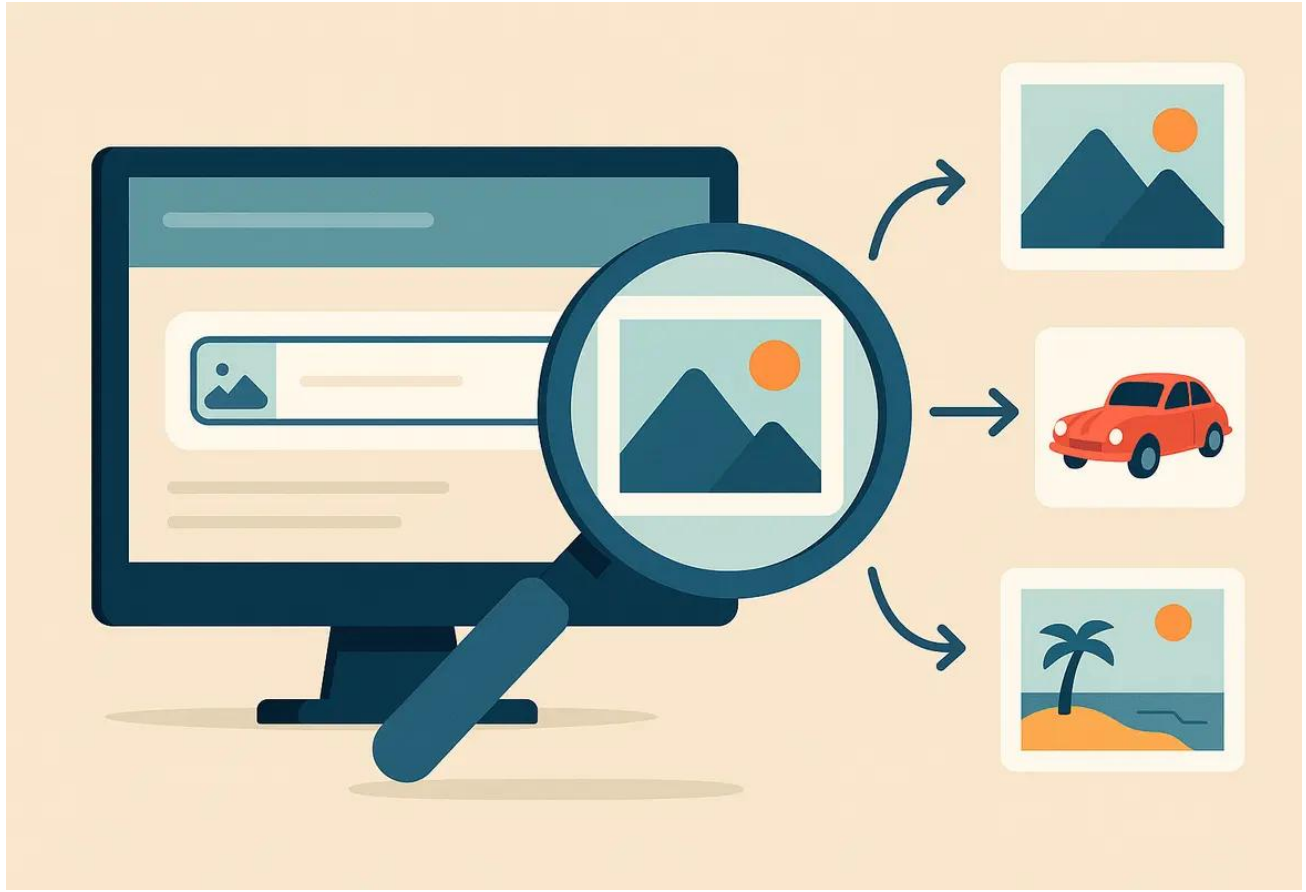
intext:"password list"
Finds pages that contain the exact phrase. Useful for spotting accidental public data dumps.

intext:"password list" filetype:txt OR filetype:csv

Reverse Image Search (RIS)

Querying the web with pixels instead of words. Algorithms analyze colors, shapes, and unique features to find where an image appears online.

- **Verification:** Determine if a profile photo is real, stolen, or stock imagery.
- **Geolocation:** Find the exact location of a photo by matching landmarks.
- **Source Tracking:** Identify the original uploader or oldest instance of a file.



Sock Puppets for Effective Online Research

When researching online, protect your privacy and security. Use virtual machines, sandboxes, and VPNs to stay safe. To avoid revealing your real identity, use Sock Puppets.

Tools:

- https://www.thispersondoesnotexist.com
- https://www.fakenamegenerator.com/

Putting it Together: How Hackers Use OSINT

Malicious actors don't need fancy zero-day exploits right away. They start with OSINT to dramatically increase the success rate of their attacks.

Step 1: Information Gathering
Collect names, job titles, family details, and personal interests from public sources.

Step 2: Building a Victim Profile
Connect the dots to understand the victim's routine, vulnerabilities, and digital identity.

Step 3: Personalized Phishing
Craft an email referencing a real-life detail (e.g., "I saw your post about X. Can you open this file for Y?") to make the attack look legitimate.

Understanding the hacker's process highlights the **ethical responsibility** of OSINT: we must treat public data with respect and focus on protecting information, not exploiting it.

Thank you

Activity:
https://nomanmunir.github.io/OSINT-Workshop