WHAT IS OSINT

AND SOME POWERFUL TOOLS RESEARCH

MALTEGO

SHODAN

Google DORKS

THE HARVESTER

What is OSINT?

Open-Source Intelligence (OSINT) is the process of collecting, analyzing, and interpreting publicly available information to produce actionable intelligence. The information is obtained legally from open sources such as websites, social media, public records, forums, satellite imagery, and news outlets.

- **Information is publicly accessible**
- **Collection is legal and ethical**
- **Focuses on analysis, not just data gathering**

Why OSINT Is Important?

Importance of OSINT:

- **Used in cybersecurity threat intelligence**
- **Supports law enforcement and counter-terrorism**
- **Critical in corporate risk assessment**
- **Applied in journalism and investigative reporting**
- **Used for military and geopolitical analysis**

OSINT Sources (Detailed Investigation)

Common OSINT Sources:

- **Search Engines (advanced Google Dorking)**

Social Media (LinkedIn, X, Instagram, TikTok)

Public Records (WHOIS, company registries)

Technical Sources (IP databases, DNS, certificates)

Dark Web (read-only analysis, no interaction)

News & Media Archives

Satellite & Geospatial Data

OSINT Tools : Academic and Practical Investigation

the Harvester

```
root@kali:~# theHarvester -d kali.org -l 500 -b duckduckgo
*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 4.4.3                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************

[*] Target: kali.org

[*] Searching Duckduckgo.

[*] No IPs found.

[*] No emails found.

[*] Hosts found: 14
---------------------
[...]

```console
```
```

theHarvester is an open-source OSINT tool primarily used for passive reconnaissance. It collects publicly available information related to domains, organizations, and individuals.

Tool for gathering e-mail accounts and subdomain names from public sources
The package contains a tool for gathering subdomain names, e-mail addresses, virtual hosts, open ports/ banners, and employee names from different public sources (search engines, pgp key servers).

Installed size: 1.94 MB
How to install: sudo apt install theharvester

Basic Email Harvesting Workflow

Define the Target Domain

You always work with a domain, not individuals.

CODE - theHarvester -d example.com -b google

Explanation

-d → Target domain

-b → Data source (search engine)

Output → Public emails linked to that domain

Use Multiple Data

CODE- theHarvester -d example.com -b google,bing,duckduckgo

For more https://pkg.kali.org/pkg/theharvester

Shodan

Shodan is a specialized search engine that indexes internet-connected devices and services.

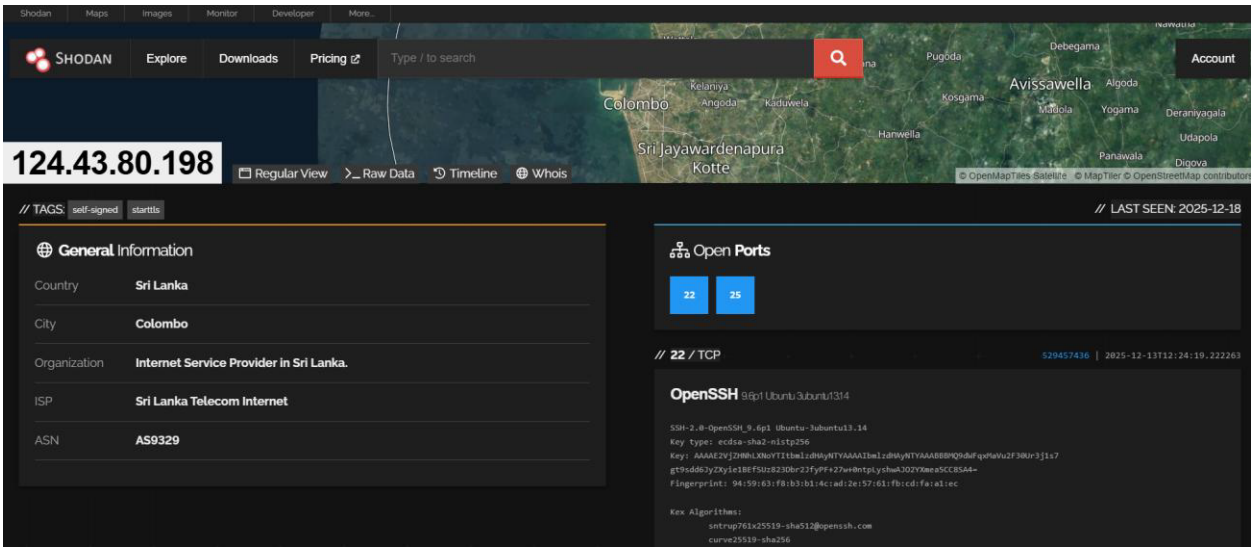
Shodan is a search engine for internet-connected devices, not for websites.

it indexes:

- Servers
- Routers
- Firewalls
- IoT devices
- Databases
- Industrial systems

Think of it like this:

- Google → searches **websites**
- Shodan → searches **devices and services**



Methodology

Shodan performs **continuous internet-wide scanning**, collecting metadata without interacting with the service beyond banner grabbing.

Yandex Images

Yandex Images is an image search engine that is exceptionally strong for OSINT, especially for:

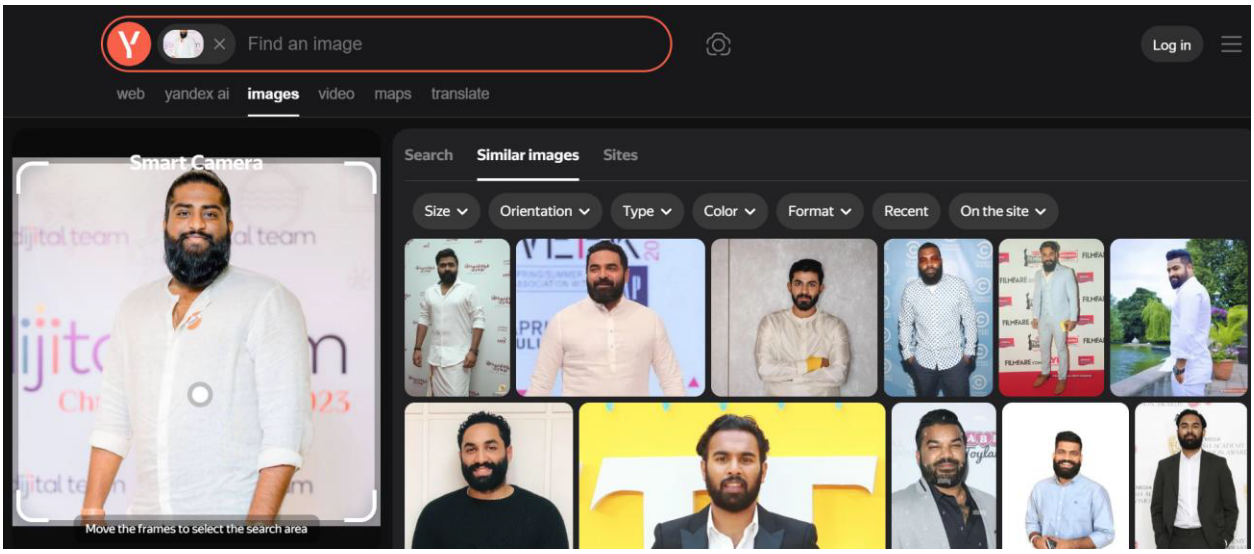
Face recognition

Location identification

Finding original image sources

Detecting reused or manipulated images

In many investigations, Yandex performs better than Google Images.



OSINT Use Cases (Very Important)

1. Fake Account Detection

Upload profile photo →
Yandex finds:

- **Same face on multiple platforms**
- **Stock image sources**
- **Older appearances**

---

2. Location Identification

Upload a photo with:

- **Buildings**
- **Street signs**
- **Landscapes**

Yandex may match:

- **City**
- **Landmark**
- **Country**
- **Similar architectural styles**

Forensic OSINT

Forensic OSINT (from *ForensicOSINT.com*) is a browser-based evidence capture platform built primarily as a Chrome extension to help investigators and analysts collect and document online information in a forensically defensible way.

It is *not* just a simple screenshot tool; it is designed to support legal, investigative, and evidentiary workflows with features that go beyond a typical screenshot extension.

Digital Evidence Capture

The central purpose of Forensic OSINT is to capture web content in detail and preserve it so it can be used in investigative reports:

Full-page, scrolling captures of web content (not only what's visible on the screen).

Video captures and downloads from platforms like YouTube, TikTok, and X.

Source code capture along with rendered content to document what was actually on the page at the point of capture.

High-clarity PDF outputs that present captures in formats suitable for reporting or evidence packets.

File hashing to prove integrity and that files have not been tampered with after capture

How to use:

1. **Enter the username(s): Input the username you want to investigate into the search box on the homepage. You can enter multiple usernames separated by commas if you're searching for more than one.**
2. **Select any category filters: Before searching, you can apply filters based on specific categories or websites to narrow down your search to particular types of platforms (e.g., social media, forums).**
3. **Initiate the search: Click the search icon or simply press CTRL+Enter to begin the search. The tool will then scour the internet for the entered username(s).**

4. Review the results: The results are displayed in two formats:

   a. **Icons on the left: These icons represent different websites where the username was found.**
   b. **Searchable table on the right: This table provides a detailed list of the websites and links to the profile or page where the username was detected.**

5. Utilize additional searches: At the bottom of the results page, document and Google searches automatically populate, using the first username from your list as the search term. This feature allows you to extend your investigation further.

https://www.forensicosint.com/ (This Tool Mainly We are Using For Documentation / Evidence Capture)

FREE TOOL FOR TO RESEARTH ABOUT TERRORISM

Global Terrorism Database

https://www.start.umd.edu/data-tools/GTD

Understand What the GTD Is

The Global Terrorism Database (GTD) is a comprehensive, open-source database of terrorist incidents worldwide from 1970 through 2020, with details on location, actors, tactics, weapons, targets, casualties, and more. It was developed for research and analysis of terrorism patterns and trends.

Search and Filter Terrorism Data

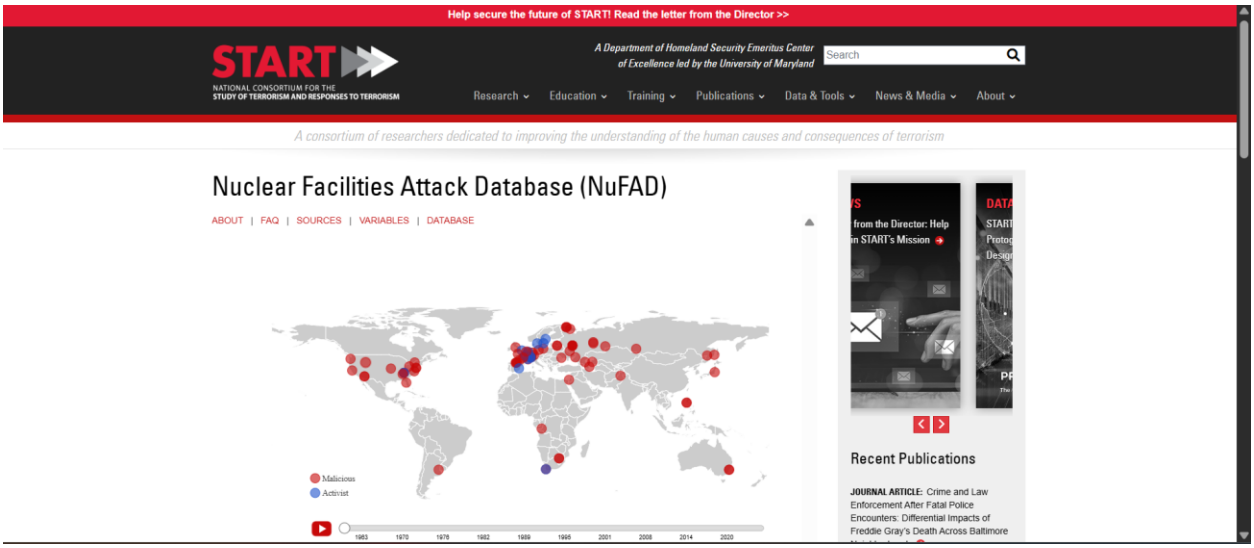
Once inside the GTD interface, you typically use a set of filters to query the data:

Common filter options you will see (interface may update over time) include:

- **Time period / Date range: Select specific years or date intervals.**
- **Region or Country: Limit incidents to a specific geography.**
- **Perpetrator group or actor name: Search by named groups.**
- **Attack type: Bombings, assassinations, kidnappings, armed assaults, etc.**
- **Target type: Government, private citizens, infrastructure, etc.**
- **Weapon type: Explosives, firearms, melee, etc.**
- **Casualty levels: Minimum fatalities or injuries.**

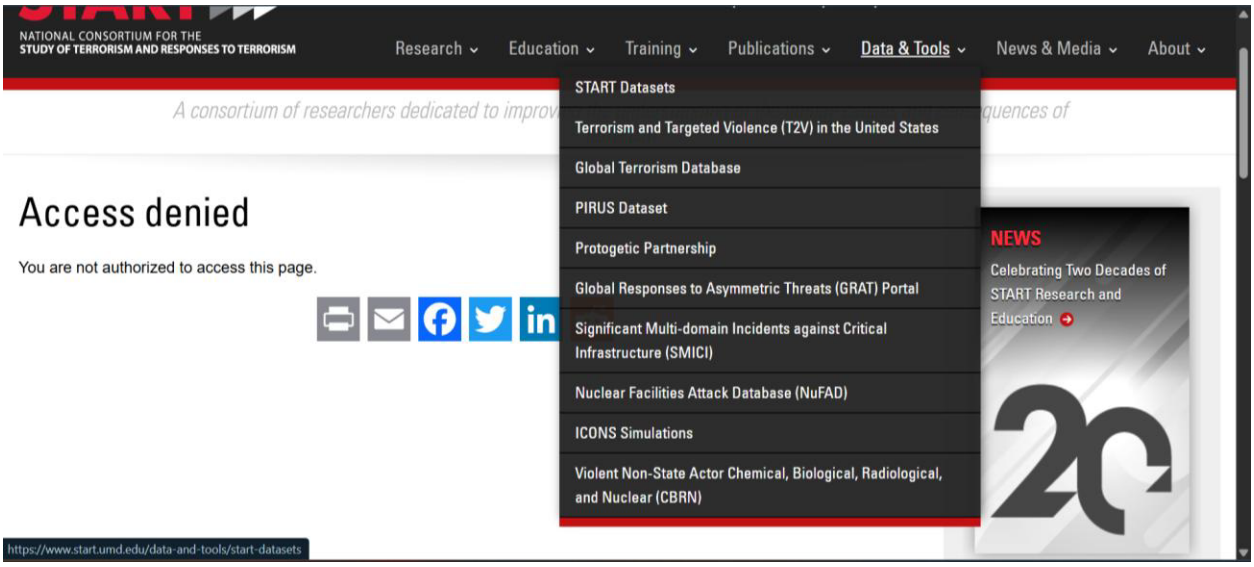
(Specific filter terminology may vary.)

Nuclear Facilities Data by using GTD .



Note – If we need to know about Regarding Terrorism Best OSINT Tool is GTD

https://www.start.umd.edu/data-tools/



UNMASK THE DIGITAL WORLD Dive deep the art Open-Source intelligence (OSINT) and unlorets hiiden in the plght. From public records to inssertane sd dvestigaws and techniues and texiniques and available used leverrages Anallyze and resaneleveerr. This guide revals how collect col s ahffemation to gain to gain unpraalled insights.

Conducted by:
Farhan
Cyber Security Student