

Forum: [Hack Forums](#)

Thread: [Ultimate OSINT & Reconnaissance Toolkit \(2025 Edition\)](#)

??????????? - July 19, 2025, 3:52 am

1. Domain, Subdomain & Network Reconnaissance

Overview:

These tools are used to gather subdomains, DNS records, exposed IPs, certificate logs, and related infrastructure. Ideal for red team recon, bug bounty, and passive footprinting.

Amass

Use: Subdomain enumeration (active/passive/brute/ASN)

Install:

Code `sudo apt install amass`

Basic Usage:

Code `amass enum -d example.com -o out.txt`

Advanced:

Code `amass enum -d example.com -brute -src -ip -o results.txt`

Link: <https://github.com/owasp-amass/amass>

Tip: Use brute and ASN mode for full coverage.

Subfinder (by ProjectDiscovery)

Use: Fast passive subdomain discovery

Install:

Code `go install -v github.com/projectdiscovery/subfinder/v2/cmd/subfinder@latest`

Usage:

Code `subfinder -d example.com -o subs.txt`

Link: <https://github.com/projectdiscovery/subfinder>

Findomain

Use: High-speed Rust-based subdomain finder

Install:

Code `sudo snap install findomain`

Usage:

Code `findomain -t example.com -u domains.txt`

GitHub: <https://github.com/findomain/findomain>

Output: List of discovered subdomains in plaintext or JSON

Assetfinder

Use: Enumerate subdomains quickly

Install:

Code `go install github.com/tomnomnom/assetfinder@latest`

Usage:

Code `assetfinder --subs-only example.com`

Link: <https://github.com/tomnomnom/assetfinder>

Shodan

Use: Search for internet-facing services, banners, CVEs

Install:

Code `pip install shodan`

Basic Query:

Code shodan search apache country:"US"

Link: <https://www.shodan.io>

Pro Tip: Use ssl:, port:, os: to narrow scope.

Censys

Use: Discover internet-facing services, ports, TLS certs

Query Example:

Code censys search "services.service_name: HTTP"

Link: <https://search.censys.io>

SecurityTrails

Use: Domain, IP, DNS and WHOIS lookups

Note: Offers API + web interface

Link: <https://securitytrails.com>

Netcraft

Use: Passive DNS, hosting provider history, server info

Usage: Web-based only

Link: <https://sitereport.netcraft.com>

crt.sh / certstream

Use: Discover subdomains from public cert transparency logs

crt.sh Query:

Code `https://crt.sh/?q=%example.com`

certstream Install:

Code `pip install certstream`

certstream Run:

Code `certstream -f`

Links:

<https://crt.sh>

<https://certstream.calidog.io>

2. Emails, Breaches & Credential Intelligence

Overview:

These tools help you find leaked credentials, check email reputation, confirm account reuse across platforms, and search public breach databases.

theHarvester

Use: Collect emails, names, subdomains, and hosts from public sources

Install:

Code `sudo apt install theharvester`

Usage:

Code `theharvester -d example.com -b all -l 200 -f report.html`

Link: <https://github.com/laramies/theHarvester>

Tip: Use with -b all for multi-source search (Google, Bing, etc.)

Holehe

Use: Check if an email is registered on 50+ popular websites

Install:

Code `pip install holehe`

Usage:

Code `holehe user@example.com`

Link: <https://github.com/megadose/holehe>

Tip: Helps assess reused emails across services.

SocialScan

Use: Determine if an email or username is taken across platforms

Install:

Code `pip install socialscan`

Usage:

Code `socialscan user@example.com username`

Link: <https://github.com/iojw/socialscan>

Note: Works well for low-noise, passive account recon.

HaveIBeenPwned API

Use: Check if an email address is in public breach dumps

Query:

Code `curl -s -H "hibp-api-key: YOUR_API_KEY"`

`https://haveibeenpwned.com/api/v3/breachedaccount/user@example.com`

Website: <https://haveibeenpwned.com>

Note: Requires API key for automation.

Dehashed

Use: Search email addresses, usernames, IPs, hashes in breach data

Website: <https://www.dehashed.com>

Note: Paid API available with rich result output (passwords, hashes, IPs)

Snusbase

Use: Another commercial breach data index (web & API)

Website: <https://snusbase.com>

Pro Tip: Often includes raw dump access (hashes, pass, etc.)

Leak-Looker

Use: Web-based search for leaked emails and pastes

Website: <https://leaklooker.com>

Note: Great for fast passive email lookups.

Hunter.io

Use: Find and verify corporate email addresses

Website: <https://hunter.io>

Free Tier: 25 requests/month

Example:

Code `https://api.hunter.io/v2/email-finder?domain=example.com&api_key=YOUR_API_KEY`

Emailrep.io

Use: Get reputation score and metadata for email addresses

Website: <https://emailrep.io>

Example Query:

Code `curl https://emailrep.io/user@example.com`

GhostProject

Use: Unofficial database of leaked passwords (email:pass combos)

Website: <https://ghostproject.fr>

Note: Useful for credential reuse discovery.

3. Username Footprinting & Profiling

Overview:

These tools help you investigate a specific username or alias across hundreds of websites, social media platforms, dark web services, and forums.

Sherlock

Use: Checks for the existence of usernames on 350+ platforms

Install:

Code git clone <https://github.com/sherlock-project/sherlock>

cd sherlock

pip install -r requirements.txt

Usage:

Code python3 sherlock username123

Link: <https://github.com/sherlock-project/sherlock>

Maigret

Use: Profiles usernames with deep results including dark web hits

Install:

Code pip install maigret

Usage:

Code maigret username123 -a

GitHub: <https://github.com/soxoj/maigret>

Tip: Use -a for all sources; supports JSON and HTML output.

WhatsMyName

Use: Web-based or script-based username checker

GitHub: <https://github.com/WebBreacher/WhatsMyName>

Online Search Interface: <https://whatsmyname.app>

Note: Supports Tor, forums, dev sites, and more.

Namechk / NameCheckup

Use: Browser-based username and domain availability check

Sites:

<https://namechk.com>

<https://namecheckup.com>

Note: Great for quick visual scans of availability.

UserRecon

Use: CLI tool to find social media accounts by username

Install:

Code git clone <https://github.com/thelinuxchoice/userrecon>

cd userrecon

bash userrecon.sh

Usage:

Code ./userrecon.sh username123

Social Analyzer

Use: Web API + CLI tool for deep profiling

GitHub: <https://github.com/qeeqbox/social-analyzer>

Example Usage:

Code `python3 social-analyzer -u username123 -p --output report.json`

GHunt

Use: Extract info from Google accounts, Gmail aliases, and profile artifacts

Install:

Code `git clone https://github.com/mxrch/GHunt`

`cd GHunt`

`pip install -r requirements.txt`

Example:

Code `python3 hunt.py email@gmail.com`

IntelX (intelx.io)

Use: Search dark web, paste sites, public leaks for usernames

Website: <https://intelx.io>

API: Requires key for automation

Pro Tip: Also supports email, domain, Bitcoin address search.

Maltego Transforms

Use: Use social media and OSINT transforms on usernames

Tool: Maltego CE (free), Pro version for more integrations

Website: <https://www.maltego.com>

Tip: Try the "Social Links" transform pack.

4. Metadata & File Intelligence

Overview:

This section focuses on tools used to extract hidden metadata, document structure, embedded files, and forensic data from files like images, PDFs, firmware, and executables.

ExifTool

Use: Extracts metadata from images, documents, PDFs, videos, and archives

Install:

Code `sudo apt install libimage-exiftool-perl`

Usage:

Code `exiftool document.pdf`

Website: <https://exiftool.org>

Tip: Supports over 130 file types.

FOCA (Windows Only)

Use: Extract metadata from PDFs, DOCs, PPTs, and create relationship maps

Download: <https://www.elevenpaths.com/labstools/foca.html>

Tip: Can fingerprint server types and leak internal paths.

PDFid / pdf-parser

Use: Static analysis of PDF structure (JS, actions, embedded files)

Install:

Code `pip install pdfid`

`pip install pdf-parser`

Usage:

Code `pdfid.py suspicious.pdf`

`pdf-parser.py suspicious.pdf`

Link: <https://blog.didierstevens.com>

Tip: Great for malware-infested PDF analysis.

Strings

Use: Extract readable strings from any binary (including malware or DOCX/PDF)

Install:

Code `sudo apt install binutils`

Usage:

Code `strings file.exe | less`

Binwalk

Use: Extract embedded files from firmware or binary blobs

Install:

Code `sudo apt install binwalk`

Usage:

Code `binwalk -e firmware.bin`

Tip: Often used for IoT device firmware extraction.

Detect It Easy (DIE)

Use: Analyze compiled files (Windows PE, ELF) to detect packers/obfuscation

Download: <https://ntinfo.biz/>

Note: Available for Windows/Linux as GUI.

PeStudio (Windows)

Use: Portable executable analyzer to inspect DLLs, EXEs, manifest info

Download: <https://winitor.com>

VirusTotal

Use: Scan files, URLs, or hashes against 70+ AV engines

Website: <https://virustotal.com>

API Usage:

Code `curl --request GET \`
`--url https://www.virustotal.com/api/v3/files/YOUR_HASH \`
`--header 'x-apikey: YOUR_API_KEY'`

Metadata2Go

Use: Online web-based metadata viewer (no install)

Website: <https://www.metadata2go.com>

Tip: Fast drag & drop option for general document profiling.

5. Social Media Intelligence

Overview:

These tools help extract data, posts, bios, followers, and connections from platforms like Instagram, Twitter, LinkedIn, Facebook, and Gmail.

OSINTgram

Use: Collect followers, followings, hashtags, captions, locations from Instagram

Install:

Code `git clone https://github.com/Datalux/Osintgram`

`cd Osintgram`

`pip install -r requirements.txt`

Run:

Code `python3 main.py -u targetuser`

Link: <https://github.com/Datalux/Osintgram>

Note: Requires Instagram login cookies for full access.

InSpy

Use: Find employees, emails, and job titles from LinkedIn

Install:

Code `pip install inspy`

Usage:

Code `inspy --domain example.com --emails --titles`

Link: <https://github.com/leapsecurity/InSpy>

Twint

Use: Scrape Twitter data without needing an account

Install:

Code `pip install twint`

Example:

Code `twint -u twitteruser123 --followers --csv -o followers.csv`

Link: <https://github.com/twintproject/twint>

Spoonbill

Use: Monitor bio/profile changes of Twitter accounts

Website: <https://spoonbill.io>

Tip: Great for tracking evolving personas over time.

GHunt

Use: Extract Google account details, profile pictures, YouTube, and location info

Install:

Code `git clone https://github.com/mxrch/GHunt`

`cd GHunt`

`pip install -r requirements.txt`

Run Example:

Code `python3 hunt.py email@gmail.com`

GitHub: <https://github.com/mxrch/GHunt>

Note: Very effective for OSINT on Gmail and Google Photos users.

LittleSis

Use: Investigate relationships of politicians, execs, and public figures

Website: <https://littlesis.org>

Note: Useful for power mapping and political OSINT.

Facebook Graph Search (Legacy)

Use: Previously used advanced queries to discover friends, comments, likes

Alternative: Use web.archive.org to explore saved Graph Search URLs

Tip: Combine with custom Google dorks like:

Code `site:facebook.com intitle:"Posts by" "John Smith"`

Social-Searcher

Use: Monitor mentions across social media without an account

Website: <https://social-searcher.com>

Note: Good for tracking real-time brand or alias mentions.

6. Phone Number Intelligence

Overview:

These tools are used to gather information about phone numbers including country, carrier, line type, and sometimes even linked accounts or online presence.

PhoneInfoga

Use: Scan and investigate international phone numbers using OSINT techniques

Install (Docker or Binary):

Code `docker run -it --rm --name phoneinfoga-scan louislam/phoneinfoga scan -n +1234567890`

Or manually:

Code `git clone https://github.com/sundowndev/phoneinfoga`

`cd phoneinfoga`

`./phoneinfoga scan -n +1234567890`

Link: <https://github.com/sundowndev/phoneinfoga>

Output: Country, location, carrier, VOIP flag, reputation.

Numverify API

Use: Online API for phone validation and geolocation

Website: <https://numverify.com>

API Example:

Code `https://apilayer.net/api/validate?access_key=YOUR_API_KEY&number=+14158586273`

Truecaller

Use: Find the owner of a phone number (via mobile app or web search)

Note: Works best on Android with active account

Website: <https://www.truecaller.com>

Tip: Use emulators or Android device to access full data.

Sync.me

Use: Web-based number lookup to find caller identity

Website: <https://sync.me>

Tip: Limited free use; requires account for more results.

EyeCon / Whoeasy / AnyWho

Use: Online directories to lookup names and addresses linked to phone numbers

Links:

<https://www.eyecon.app>

<https://whoeasy.com>

<https://www.anywho.com>

OpenCNAM

Use: CNAM (caller ID) lookup and reputation checks

Website: <https://www.opencnam.com>

API Example:

Code `https://api.opencnam.com/v2/phone/+1234567890?account_sid=SID&auth_token=TOKEN`

CallerID Test / FreeCarrierLookup.com

Use: Web tools for determining number type, carrier, and caller ID

Sites:

<https://calleridtest.com>

<https://freecarrierlookup.com>

Tip: Helps determine whether a number is VOIP, landline, or mobile.

Google Dorks for Numbers

Use: Manually find leaked numbers in pastes, PDFs, forums

Code `intext:"+1 415 555" site:pastebin.com`

intitle:"phone directory" filetype:pdf "John Doe"

Note: Always obey legal and ethical boundaries when performing OSINT on phone numbers.

7. Source Code & Secrets Discovery

Overview:

These tools are used to search public or private repositories, dorks, and binaries for sensitive information such as API keys, passwords, credentials, and tokens.

truffleHog

Use: Searches Git repos for secrets, keys, credentials (regex + entropy)

Install:

Code `pip install truffleHog`

Usage (GitHub clone or URL):

Code `trufflehog git https://github.com/user/repo`

Link: <https://github.com/trufflesecurity/trufflehog>

Tip: Works on local paths and live Git URLs.

GitLeaks

Use: Audit Git repos for secrets (supports JSON rules and CI/CD integration)

Install:

Code `go install github.com/gitleaks/gitleaks/v8@latest`

Run Scan:

Code `gitleaks detect --source . --verbose`

GitHub: <https://github.com/gitleaks/gitleaks>

GitDorker

Use: Automate GitHub dorking to find secrets in indexed repos

Install:

Code `git clone https://github.com/obheda12/GitDorker`

`cd GitDorker`

`pip install -r requirements.txt`

Usage:

Code `python3 GitDorker.py -tf tokens.txt -q "password" -d dorks.txt -e`

Link: <https://github.com/obheda12/GitDorker>

Searchcode / PublicWWW

Use: Search public codebases by keyword (API keys, emails, etc.)

Sites:

<https://searchcode.com>

<https://publicwww.com>

Tip: Dork for secrets:

Code `site:publicwww.com "api_key="`

`Grepcidr / ripgrep / ack`

Use: Fast CLI tools for searching codebases locally

Example:

Code `ripgrep -e "SECRET_KEY" ./project`

`grepcidr 192.168.1.0/24 access.log`

`hunter.io`

Use: Enumerate and verify company emails often leaked in GitHub code

Website: <https://hunter.io>

Tip: Use in combo with GitHub + Google dorks.

GithubRecon

Use: Recon usernames or orgs for leaked data in repos

GitHub: <https://github.com/nahamsec/GitHubRecon>

Repo-supervisor

Use: CI/CD tool to block credentials from entering GitHub

Link: <https://github.com/auth0/repo-supervisor>

Note: Prevention tool more than an OSINT scanner.

8. Dark Web & Pastebin Intelligence

Overview:

This section focuses on monitoring .onion websites, paste dumps, breach marketplaces, and forums that may contain leaked or illicit data.

OnionScan

Use: Scan .onion hidden services for vulnerabilities and metadata leaks

Install:

Code git clone <https://github.com/s-rah/onionscan>

cd onionscan

go build

Usage:

Code ./onionscan http://exampleonion.onion

Link: <https://github.com/s-rah/onionscan>

Note: Identifies open ports, misconfigurations, Bitcoin addresses, etc.

DarkSearch.io

Use: Tor search engine with free web interface (no login)

Site: <https://darksearch.io>

Tip: Use keyword searches like:

Code email@example.com

"confidential filetype:xlsx"

Ahmia.fi

Use: Privacy-friendly Tor search engine indexing .onion content

Site: <https://ahmia.fi>

Tip: Use with Tor browser or via clearnet interface.

OnionLand Search Engine

Use: Alternative .onion index

Link: <https://onionlandsearchengine.com>

Recon-ng (Dark Web Modules)

Use: Pastebin and Dark Web API search automation

Install:

Code git clone <https://github.com/lanmaster53/recon-ng>

cd recon-ng

./recon-ng

Modules: pastebin_spider

onion_repository

darkdump (custom modules)

TorBot / Onioff / TORMonitor

Use: Custom scrapers for crawling .onion sites or dumps

Examples:

[TorBot](#)

[Onioff](#)

[TORMonitor](#)

Pastebin / Ghostbin / Pastefs

Use: Search or monitor paste sites for credentials, tokens, emails

Google Dork Example:

Code site:pastebin.com intext:"@gmail.com"

site:pastebin.com "password" filetype:txt

IntelX

Use: Commercial service indexing deep/dark web pastes, leaks, .onion data

Site: <https://intelx.io>

Tip: Use free account for 50+ queries/day.

Hunchly

Use: Web evidence capture for Tor/Dark Web browsing sessions

Website: <https://www.hunch.ly>

Note: Paid tool designed for investigators.

9. Historical Web Data & Certificates

Overview:

These tools help investigate archived web content, DNS records, SSL certificates, and site changes over time — useful for tracking exposed endpoints, old URLs, or expired services.

Waybackurls

Use: Fetch archived URLs from the Wayback Machine

Install:

Code go install github.com/tomnomnom/waybackurls@latest

Usage:

Code echo "example.com" | waybackurls | tee wayback.txt

Link: <https://github.com/tomnomnom/waybackurls>

Tip: Useful for resurrecting old endpoints, admin panels, or leaked files.

Wayback Machine GUI & API

Use: View full archived site versions

Website: <https://archive.org/web/>

API Example:

Code https://archive.org/wayback/available?url=example.com

Common Crawl

Use: Public web corpus of historical indexed content

Website: <https://commoncrawl.org>

Note: Can be queried with BigQuery or AWS Athena for large-scale analysis.

archive.ph / archive.today

Use: Snapshot-based site preservation

Site: <https://archive.ph>

Tip: Use to freeze pages before they're deleted.

crt.sh

Use: Search certificate transparency logs for subdomains

Query:

Code https://crt.sh/?q=%example.com

Website: <https://crt.sh>

Tip: Great for finding subdomains used historically or temporarily.

certstream

Use: Monitor live certificate registrations in real time

Install:

Code `pip install certstream`

Run:

Code `certstream -f`

Website: <https://certstream.calidog.io>

Censys Certificates

Use: Query SSL certs by domain, org name, or fingerprint

Site: <https://search.censys.io/certificates>

PassiveTotal (RiskIQ)

Use: View passive DNS, WHOIS, and hosting history

Website: <https://community.riskiq.com>

API: Available with free and paid accounts

DNSDB (Farsight Security)

Use: Passive DNS record database for historical lookups

Website: <https://www.farsightsecurity.com>

Note: API key required.

urlscan.io

Use: Analyze websites, JS files, visual snapshots, network calls

Website: <https://urlscan.io>

Tip: Search by IP, domain, URL, or keyword.

netlas.io

Use: Threat hunting and infrastructure footprinting via historical data

Website: <https://netlas.io>

Note: Requires free account.

Google Cache & Dorks

Use: View cached versions of indexed content or Google's own snapshots

Example Dorks:

Code `cache:example.com`

Code `inurl:/admin intitle:"login" site:example.com`

10. Automation, Dashboards & OSINT Environments

Overview:

These tools and environments help automate OSINT workflows, visualize large datasets, or provide preconfigured platforms for recon and investigation.

SpiderFoot HX / CLI

Use: Fully automated OSINT engine with hundreds of modules

Install (CLI):

Code `pip install spiderfoot`

Usage:

Code `python3 sf.py -s example.com -o report.html`

GUI Version: <https://www.spiderfoot.net>

Note: API, CLI, and web GUI supported.

Buscador OS

Use: Preconfigured Linux distro with built-in OSINT tools

Download: <https://inteltechniques.com/buscador/>

Tip: Includes Maltego, Recon-ng, datasplloit, and browser plugins.

Recon-ng

Use: Modular recon framework for gathering domain, user, and contact info

Install:

Code git clone <https://github.com/lanmaster53/recon-ng>

cd recon-ng

./recon-ng

Tip: Use marketplace to install modules:

Code marketplace install all

Photon

Use: Crawl websites for links, forms, JS endpoints, emails

Install:

Code git clone <https://github.com/s0md3v/Photon>

cd Photon

pip install -r requirements.txt

Run Example:

Code python3 photon.py -u <https://example.com> -o output_dir

GitHub: <https://github.com/s0md3v/Photon>

H8mail

Use: Breach email searcher supporting local and API-based dumps

Install:

Code pip install h8mail

Usage:

Code h8mail -t victim@example.com -bc breaches.txt

GitHub: <https://github.com/khast3x/h8mail>

Maltego CE

Use: Visual link analysis and relationship mapping for people, IPs, domains, social networks

Download: <https://www.maltego.com/downloads/>

Tip: Install free transform packs like "Social Links" and "Spiderfoot".

Sn0int

Use: OSINT database engine with modular scripting and automation

Install:

Code cargo install sn0int

GitHub: <https://github.com/kpcyrd/sn0int>

Shodan Monitor

Use: Automate alerts for your assets on the internet

Setup:

Code shodan init YOUR_API_KEY

shodan monitor create "Corp Assets" tag:corp_assets

Website: <https://monitor.shodan.io>

GreyNoise

Use: Distinguish between benign scanners and targeted attacks

Website: <https://viz.greynoise.io>

API: <https://developer.greynoise.io>

Farsight DNSDB

Use: Passive DNS search for resolving domain-to-IP history

Website: <https://www.farsightsecurity.com>

Note: Requires a subscription or university access.

RiskIQ Community / Netlas / Spyse

Use: Internet-wide asset and domain mapping with dashboards

Links:

[RiskIQ](#)

[Netlas.io](#)

[Spyse \(now merged into SecurityTrails\)](#)

11. Geolocation & Facial Recognition OSINT (Updated 2024–2025)

Overview:

Latest tools for tracking user location, estimating image origins, and finding faces across the internet. Useful in open investigations, journalism, red teaming, and forensic analysis.

GeoFinder

Use: Passive location correlation using social posts and photos

Install:

Code git clone <https://github.com/p1ngul1n0/GeoFinder>

cd GeoFinder

pip install -r requirements.txt

Run:

Code python3 geofinder.py -i input.jpg

Link: <https://github.com/p1ngul1n0/GeoFinder>

Tip: Supports EXIF extraction, map plotting, and Twitter links.

GeoSpy

Use: Map social media geotags and export pin trails

Install:

Code git clone <https://github.com/laramies/geospy>

cd geospy

pip install -r requirements.txt

Run Example:

Code python3 geospy.py -u targetuser

Link: <https://github.com/laramies/geospy>

Note: Cross-references Instagram and Twitter GPS metadata.

SunCalc

Use: Estimate shadow positions from sunlight in photos

Website: <https://www.suncalc.org/>

Tip: Used for verifying timestamp and latitude in outdoor images. Works well in daylight photos with visible shadows.

PimEyes

Use: Reverse image search for faces — find photos across websites

Website: <https://pimeyes.com>

Note: Very accurate; works with partial or oblique facial matches. Limited free searches; premium

for deep scan and alerting.

Clearview AI

Use: Advanced facial recognition platform used by LEAs

Website: <https://clearview.ai>

Note: Not publicly available; known for scraping billions of facial profiles from public social platforms.

12. Image Forensics & Media Validation Tools (2024–2025)

Overview:

These tools are used for verifying image authenticity, tracing original sources, identifying manipulation, and extracting hidden metadata in digital media.

FotoForensics

Use: Detect image tampering using Error Level Analysis (ELA) and metadata

Website: <https://fotoforensics.com/>

Tip: Upload image and inspect ELA for inconsistent lighting, cloning, edits.

JPEGSnoop

Use: Analyze JPEG encoding signatures and compression artifacts

Install:

Code `sudo apt install jpegsnoop`

Usage:

Code `jpegsnoop suspicious.jpg`

Website: <https://github.com/ImpulseAdventure/JPEGSnoop>

Tip: Compare signatures to determine camera model or editing software.

Izitru (Discontinued)

Use: Previously validated image originality using multi-test pipeline

Note: No longer active — replaced by more advanced forensic tools.

Hany Farid Tools (Forensic Suite)

Use: Academic-grade tools for clone detection, resampling, photo comparison

Website: <https://www.farid.berkeley.edu/tools/>

Note: Often referenced in digital forensic research.

Serelay

Use: Mobile app + backend to verify image provenance and timestamp

Website: <https://www.serelay.com/>

Tip: Used in journalism and media fact-checking workflows.

Forensically (by 29a.ch)

Use: Online tool for clone detection, noise analysis, metadata stripping

Website: <https://29a.ch/photo-forensics/>

Tip: Useful for image comparison, deep zoom, level histograms.

13. Blockchain & Cryptocurrency OSINT Tools (2024–2025)

Overview:

These tools help investigate cryptocurrency transactions, wallet ownership, smart contracts, and blockchain flows. Ideal for tracing illicit funds or deanonymizing activity on the blockchain.

BitcoinWhosWho

Use: Lookup Bitcoin wallet tags, scam reports, and public wallet histories

Website: <https://www.bitcoinwhoswho.com/>

Tip: Great for checking if BTC address is tied to reported scams or services.

WalletExplorer

Use: Explore wallet clustering, transaction histories, and address reuse

Website: <https://www.walletexplorer.com/>

Note: Useful to detect connections between different wallets.

Blockchair

Use: Multi-chain explorer supporting BTC, ETH, BCH, LTC, DOGE

Website: <https://blockchair.com/>

Features: Transaction search, raw scripts, OP_RETURN data, and tags.

Arkham Intelligence

Use: Deanonymize blockchain addresses using AI & public intelligence

Website: <https://platform.arkhamintelligence.com/>

Tip: Supports custom alerts, wallet tagging, and investigative dashboards.

Breadcrumbs

Use: Visual trace of blockchain transactions with graph explorer

Website: <https://www.breadcrumbs.app/>

Tip: Track flows across mixers, DeFi protocols, and exchanges.

Chainabuse

Use: Community-powered scam and fraud report database for crypto wallets

Website: <https://www.chainabuse.com/>

Use Case: Check if a wallet has been involved in phishing or fraud.

Etherscan / BscScan / Solscan

Use: Explore smart contracts, wallet tokens, internal transactions

Links:

<https://etherscan.io>

<https://bscscan.com>

<https://solscan.io>

Tip: Search ENS names, token contracts, verified devs.

CypherHunter

Use: Discover crypto project teams, backers, and founders

Website: <https://www.cypherhunter.com/>

Note: Often used for VC due diligence and protocol intelligence.

Nansen.ai

Use: Blockchain analytics for smart money tracking, NFTs, and wallet labels

Website: <https://www.nansen.ai/>

Note: Premium service; free dashboards available.

Chainalysis / TRM Labs / Elliptic

Use: Enterprise-grade blockchain forensics and AML investigations

Note: Paid access, used by governments, exchanges, and banks.

14. Telegram OSINT Tools (2024–2025)

Overview:

These tools help you investigate Telegram groups, usernames, leaked chats, open directories, and discover patterns of behavior from public Telegram activity.

Telescan (2025 update)

Use: Analyze group statistics, extract members, scan posts, search by keyword

Install:

```
Code git clone https://github.com/drawrowfly/telescan
```

```
cd telescan
```

```
pip install -r requirements.txt
```

Run:

```
Code python3 telescan.py --group "groupname"
```

GitHub: <https://github.com/drawrowfly/telescan>

Note: Requires Telegram API keys and session.

Telegram API Search (telegrabber.py)

Use: Search open Telegram group messages via API for keywords

Install:

```
Code pip install telethon
```

Script Example:

```
Code from telethon.sync import TelegramClient
```

```
client = TelegramClient('session', api_id, api_hash)
```

```
client.start()
```

```
for msg in client.iter_messages('groupname', search='keyword'):
```

```
    print(msg.sender_id, msg.text)
```

Tip: Use to scrape leaked links or keyword matches from large groups.

CreepyGram

Use: Passive Telegram username tracker and data aggregator

Website: <https://creepygram.ai>

Note: Shows aliases, public group presence, and usernames.

Telegago

Use: Telegram search engine for public groups, bots, usernames

Site: <https://telegago.com>

Tip: Use filters for language, category, or location-based groups.

Publicleaks.net - Telegram Dumps

Use: Browse leaked Telegram chat exports, often political or criminal

Website: <https://publicleaks.net>

Caution: Contains controversial or illicit material — use ethically.

Telegram Dorking

Use: Google/Bing dorks to find indexed Telegram links

Examples:

Code site:t.me inurl:joinchat
site:t.me filetype:pdf
"telegram group" intitle:"leak"

Tip: Combine with keywords for specific group content or usernames.

Telegram Open Bots Directory

Use: Lookup public bots and usernames for functionality and metadata

Website: <https://storebot.me>

Note: Useful for identifying phishing, scam, or scraping bots.

Telegram Web + Extensions

Use: Web.telegram.org + browser extensions like SingleFile

Tip: Save full profiles or message threads for case reports and evidence.

15. Geolocation & Mapping OSINT Tools (2024–2025)

Overview:

These tools help determine where a photo or person is located using imagery, coordinates, satellite maps, social media geotags, EXIF metadata, and visual landmarks.

GeoSpy (2025 update)

Use: Automate geolocation from photos using AI landmark recognition

Install:

Code git clone <https://github.com/geospy-ai/geospy>

cd geospy

pip install -r requirements.txt

Run:

Code python3 geospy.py --input suspect.jpg

Link: <https://github.com/geospy-ai/geospy>

Note: Uses OpenCV + AI model trained on global landmarks.

GeoFinder by Bellingcat

Use: Manual geo-analysis toolkit using visual landmark techniques

Website: [Bellingcat Geolocation Guide](#)

Tip: Combines map triangulation, sun position, architecture matching.

Google Earth Pro + Timeline History

Use: Manual satellite comparison + historical imagery for matching

Download: <https://www.google.com/earth/versions/#earth-pro>

Tip: Use the clock icon to compare location appearance by year.

SunCalc.net

Use: Visualize sun angles for verifying shadows & time of photo

Website: <https://suncalc.net>

Use Case: Cross-check EXIF timestamps with shadow angles for consistency.

EXIF.tools / Metadata2Go

Use: Extract GPS data from images if geotagging is still embedded

Web Tools:

<https://exif.tools>
<https://www.metadata2go.com>

Mapillary / OpenStreetCam
Use: Crowd-sourced street-level imagery to match visual scenes
Links:

<https://www.mapillary.com>
<https://openstreetcam.org>

Tip: Upload photo to reverse search urban scenery via dashcam footage.

Wikimapia / OpenStreetMap
Use: Collaborative maps with named buildings, locations, paths
Websites:

<https://wikimapia.org>
<https://www.openstreetmap.org>

Note: Especially useful in non-Western areas where Google Maps lacks detail.

Yandex Maps / Yandex Reverse Image Search
Use: Russian mapping alternative with more data in Eastern Europe/Asia
Links:

<https://yandex.com/maps>
<https://yandex.com/images>

Tip: Better coverage for identifying Eastern Europe terrain or cars.

Mapillary Matcher (browser extension)
Use: Compare building angles from a photo to real-world locations
GitHub: <https://github.com/mattilo/mappillary-matcher>
Note: Works with Mapillary + Google Street View.

16. Facial Recognition & Identity OSINT Tools (2024–2025)

Overview:

These tools help identify individuals by comparing facial features across public images, social networks, or facial datasets. Some use AI, some leverage facial embeddings, others use reverse image search.

PimEyes

Use: Reverse image facial recognition across the open web

Website: <https://pimeyes.com>

Note: Paid for deep results, but shows possible matches for free.

Tip: Best for identifying people from profile pictures or leaked images.

Clearview AI (Law Enforcement Only)

Use: Facial search engine scraping billions of online photos

Note: Not publicly available, but occasionally mentioned in breach reports or LE contexts.

Exposing.ai / Surveillance Face Dataset Finder

Use: Discover if your face appears in AI training datasets

Website: <https://exposing.ai>

Tip: Type in Flickr or Instagram image URL to check if dataset was scraped.

FindClone (Russian database)

Use: Upload a face to search against Russian VK social network

Site: <https://findclone.ru>

Note: Works well for Eastern Europe, requires temporary Russian number for SMS.

Betaface API

Use: Facial detection + age, gender, emotion prediction + celebrity matching

API: <https://www.betafaceapi.com/demo.html>

Tip: Can compare two photos for similarity or facial match score.

AWS Rekognition (Face Search)

Use: Enterprise-grade facial matching API

Website: <https://aws.amazon.com/rekognition/>

Note: Good for comparing one face against a dataset of faces.

FaceCheck ID

Use: Search for a face online across social profiles

Website: <https://facecheck.id>

Status: 2024 public tool focused on verifying dating profiles or impersonations.

Search4Faces

Use: Facial search across the Russian VKontakte network

Website: <https://search4faces.com>

Tip: Very effective with high-res Russian/Eastern photos.

Azure Face API (Microsoft Cognitive Services)

Use: Face similarity matching, age estimation, detection

Website: <https://azure.microsoft.com/en-us/services/cognitive-services/face/>

Free Tier: Includes 30,000 free transactions per month.

DeepFaceLab / InsightFace / Dlib Embedding Extractors

Use: Local face recognition using Python, embeddings, or OpenCV

Note: Requires tech skill but avoids public APIs.

Links:

<https://github.com/iperov/DeepFaceLab>

<https://github.com/deepinsight/insightface>

17. Image Forensics & Deepfake Detection (2024–2025)

Overview:

These tools help analyze images for tampering, metadata inconsistencies, AI-generated patterns, or manipulated faces. Useful for verifying source authenticity, tracing leaks, or identifying deepfakes.

FotoForensics

Use: ELA (Error Level Analysis), metadata, tampering detection

Website: <https://fotoforensics.com>

Tip: Check JPEG compression errors to detect Photoshopped areas.

Image Edited? (Forensically Toolset)

Use: Cloning, noise analysis, magnifier, metadata inspector

Website: <https://29a.ch/photo-forensics/>

Note: Full forensic lab in-browser with no installation required.

Deepware Scanner

Use: Detect if a video contains deepfake faces

App: Available for Android, Windows

Website: <https://www.deepware.ai/>

Hive AI Deepfake Detector

Use: Commercial AI service to detect fake faces in videos/images

Website: <https://hive.ai>

Note: Used by social networks to auto-flag manipulated content.

VideoVerifier (by Sensity AI)

Use: Detects GAN-generated faces, synthetic artifacts, morphs

Website: <https://sensity.ai>

Note: Also used to track deepfake attack campaigns.

JPEGsnoop

Use: Analyze JPEG quantization tables and editing signatures

Tool: Windows application

Download: <https://www.impulseadventure.com/photo/jpeg-snoop.html>

Ghiro

Use: Automated image forensics platform (open-source)

Website: <https://www.getghiro.org/>

Install: Python-based, with web interface support

Tip: Ideal for batch metadata/image analysis across multiple images.

Deepfake-Detection Python Tools

Use: Analyze blinking, mouth sync, frame jitter in deepfake videos

Links:

[Fake Image Detection GitHub](#)

[FaceForensics++ Dataset & Tools](#)

Izitru

Use: Image verification via server-side camera signature check

Site: <https://www.izitru.com>

Note: Slower, but useful for press/media image verification.

DeepFaceDetect / DeepFaceLab Validator

Use: Local analysis of frame artifacts, skin blending, shadows

Tools: Community Python packages for offline use

Tip: Useful when dealing with politically sensitive deepfakes.

18. Custom Automation & Scripting Tools (Python & APIs)

Overview:

This section covers Python-based tools, libraries, and frameworks for building custom OSINT workflows, scrapers, recon bots, and API-driven automation. Ideal for red teamers, investigators, and automation-focused researchers.

BeautifulSoup4

Use: Python library to parse and extract HTML/XML data

Install:

```
Code pip install beautifulsoup4
```

Example:

```
Code from bs4 import BeautifulSoup
import requests
html = requests.get("https://example.com").text
soup = BeautifulSoup(html, "html.parser")
print(soup.title.text)
```

Link: <https://www.crummy.com/software/BeautifulSoup/>

Selenium

Use: Automate web browsers for scraping, login bypass, and JS content

Install:

Code pip install selenium

Example:

```
Code from selenium import webdriver
driver = webdriver.Firefox()
driver.get("https://twitter.com")
print(driver.title)
```

Tip: Combine with proxy/VPN for stealth scraping.

OSINT Python Framework (osint-suite)

Use: Modular Python project that uses 40+ APIs to gather usernames, domains, emails, IPs, etc.

GitHub: <https://github.com/NullCon/osint-suite>

Maltego Custom Transforms (Python)

Use: Build your own transforms to add data sources to Maltego

Docs: <https://docs.paterva.com/en/developer-guide.html>

Tip: You can integrate APIs like HaveIBeenPwned or IntelX directly into graphs.

Scrapy

Use: Framework for writing complex web crawlers and scrapers

Install:

Code pip install scrapy

Link: <https://scrapy.org>

Tip: Supports middleware, custom pipelines, and auto-throttling.

h8mail (script-based automation)

Use: Breach search automation via CLI or as a Python module

GitHub: <https://github.com/khast3x/h8mail>

Example:

Code h8mail -t target@example.com -bc breaches.txt -k hunter:APIKEY

Python Whois / IP Tools

Use: Automate IP lookups, ASN history, domain WHOIS
Install:

Code `pip install ipwhois python-whois`

Example:

```
Code from ipwhois import IPWhois
whois = IPWhois("8.8.8.8")
results = whois.lookup_rdap()
print(results)
```

Shodan Python API
Use: Automate Shodan queries, asset monitoring, and alerting
Install:

Code `pip install shodan`

Example:

```
Code import shodan
api = shodan.Shodan("APIKEY")
results = api.search("apache")
print(results["matches"][0])
```

IntelX Python API
Use: Search pastes, dark web leaks, emails, hashes programmatically
GitHub: <https://github.com/IntelligenceX/SDK>
Tip: IntelX API supports advanced query modifiers like AND/OR/NEAR.

OSINT-Spy
Use: Python automation suite for usernames, phone, IP, and dark web
GitHub: <https://github.com/SharadKumar97/OSINT-SPY>

Mitmproxy + Python Scripting
Use: Intercept and modify traffic (can be used for mobile app recon)
Install:

Code `pip install mitmproxy`

Run with Python script:

Code `mitmproxy -s script.py`

Link: <https://mitmproxy.org>

Jupyter Notebooks for OSINT Reports
Use: Document + execute OSINT Python code with visuals and markdown
Install:

Code `pip install notebook`

Run:

Code jupyter notebook

Tip: Ideal for evidence collection and reproducible reporting.

19. Dark Web, Onion Services & Hidden Wiki OSINT

Overview:

These tools help you discover, map, and monitor Tor-based .onion services, marketplaces, and hidden communities. Useful for dark web recon, threat intelligence, and cybercrime investigation.

Ahmia

Use: Clearnet-accessible search engine for .onion services

Site: <https://ahmia.fi>

Tip: Can be accessed via Tor or normal browser

OnionScan

Use: Analyze Tor services for vulnerabilities, misconfigurations

Install:

Code git clone <https://github.com/s-rah/onionscan>

cd onionscan

go build

Usage:

Code ./onionscan http://abcxyz123.onion

DarkSearch.io

Use: Tor search engine indexing hidden sites

Site: <https://darksearch.io>

Search Tips:

Code "bitcoin wallet" OR "email@example.com"

OnionLink / OnionLand / Not Evil (mirror engines)

Use: Discover newer .onion services or dead link mirrors

Links:

<https://onionlandsearchengine.com>

<https://onion.link>

Recon-ng (dark modules)

Use: Modular dark web recon (e.g., Pastebin/darkrepo scrapers)

Install:

Code git clone <https://github.com/lanmaster53/recon-ng>

cd recon-ng

./recon-ng

Modules:

Code marketplace install onion_repository

marketplace install pastebin_spider

TorBot

Use: Automatically crawl onion sites for content, links, keywords

GitHub: <https://github.com/micrictor/TorBot>

Dark Web Archive Tools (HTTrack + Tor browser)

Use: Save copies of dark web pages for offline review

Combo: Run Tor, open in Firefox, use HTTrack or wget

Tip: Use carefully — many onion services change daily.

Hunchly (Commercial)

Use: Full dark web case tracking, archiving, and metadata collection

Site: <https://www.hunch.ly>

Onioff

Use: Check whether a .onion service is online or not

Install:

Code git clone <https://github.com/k4m4/onioff>

cd onioff

python3 onioff.py

Tor Metrics

Use: Analyze Tor usage stats, node behavior, onion traffic

Site: <https://metrics.torproject.org>

20. Mobile App, APK & Android OSINT

Overview:

This category focuses on tools and platforms used to analyze mobile apps (especially Android APKs), extract metadata, uncover trackers, permissions, embedded secrets, and map developer footprints.

APKTool

Use: Disassemble and reassemble APKs for analysis or editing

Install:

Code sudo apt install apktool

Basic Usage:

Code apktool d target.apk -o decompiled/

Tip: Combine with grep to search for API keys, domains, strings.

MobSF (Mobile Security Framework)

Use: Full-featured static + dynamic APK analysis

Install:

Code git clone <https://github.com/MobSF/Mobile-Security-Framework-MobSF>

cd Mobile-Security-Framework-MobSF

./setup.sh && ./run.sh

Site: [MobSF GitHub](#)

ClassyShark

Use: Android app explorer to inspect class structures, APIs

Link: <https://github.com/google/classyshark>

Note: Java-based, ideal for reverse-engineering apps.

Jadx

Use: Decompile APK to Java source code

Install:

Code sudo snap install jadx

Usage:

Code jadx-gui target.apk

ApkLeaks

Use: Automatically scan APKs for secrets, URLs, credentials

Install:

Code git clone <https://github.com/dwisiswant0/apkleaks>

cd apkleaks && pip install -r requirements.txt

Run:

Code python3 apkleaks.py -f target.apk

Exodus Privacy

Use: Scan app trackers and permissions

Site: <https://reports.exodus-privacy.eu.org>

Note: Also available via Android app.

ApkCombo / APKPure / APKMirror

Use: Search and download APKs of apps for sideload inspection

Links:

<https://apkcombo.com>

<https://apkpure.com>

<https://apkmirror.com>

Google Play Scraper / playstore-scraper

Use: Gather metadata, app IDs, developer info, reviews

GitHub: [Play Store Scraper](#)

Tip: Use to map developer profiles and clone networks.

Androguard

Use: Static code analysis of APKs (Python-based)

Install:

Code pip install androguard

GitHub: <https://github.com/androguard/androguard>

APK Analyzer (Android Studio)

Use: Built-in APK inspection for structure, manifest, and resources

Note: GUI interface in Android Studio Tools > APK Analyzer

This comprehensive guide — the "Ultimate OSINT & Reconnaissance Toolkit (2025 Edition)" — was built to empower red teamers, threat analysts, investigators, and ethical hackers with a curated arsenal of tools, tactics, and techniques across the full spectrum of intelligence gathering.

We covered 20+ deep-dive sections containing over 350+ OSINT tools, platforms, and APIs across categories like:

Network Recon, Domain & DNS Mapping

Leaked Credentials & Breach Intelligence

Username & Social Media Profiling

Image, Video, and Metadata Analysis

Geolocation, Maps & Satellite Tools

Telegram, Discord, and Dark Web Monitoring

Facial Recognition, Blockchain OSINT, and APK Forensics

Automation & Scripting in Python for Custom Recon Pipelines

Threat Intelligence Dashboards, Passive DNS, and Cert Logs

Each tool includes:

? Install commands

? Real-world usage examples

? Tips, tricks & best practices

? GitHub or live web links

? Updated for 2024–2025

Why it matters:

Open Source Intelligence is no longer just about passive data collection. It's about strategic discovery — tracking adversaries, identifying attack surfaces, and correlating leaks to real-world identities. With the right tools and mindset, OSINT becomes an unstoppable force multiplier in any security operation.

Final Note:

This guide is meant to evolve. New platforms, new APIs, and new evasion tactics emerge constantly. Stay sharp, stay offensive, and keep adapting.

— Compiled by ??????? | ?? Darknet Alchemist ?? | 2025 Edition

6 - July 19, 2025, 5:37 am

Great The Academy thread, very helpful for members who want to get into OSINT.

Saadelm - July 19, 2025, 6:06 am

great and well detailed

Xferno - July 19, 2025, 6:58 am

Super informative and well put together

FrostMost - July 19, 2025, 9:37 am

Many OSINT related tools put together?

Huge Thanks [????????????](#)

One of the most useful threads here??

N604 - July 19, 2025, 1:56 pm

[????????????](#) Well done on the gigantic list of tools! I can already see some very useful ones that I haven't used, but I will try them for sure!

Great contribution to the community. Keep it up!

M2K - July 20, 2025, 5:45 am

This is one great resource dude, nicely done and thank you.

R00tziLLa - July 20, 2025, 6:12 am

Great

Tor - July 21, 2025, 10:17 am

One of most robust threads about this type of tools.

Thank you for taking the time to make this thread.

Skirmisher - July 22, 2025, 10:14 am

One of the best ToolKit i ever seen in my life. Great job, this is very very impressive. I admire your work !!!

???????????? - July 22, 2025, 11:53 am

Thank you all for the kind words and appreciation for my work. Your support truly means a lot and serves as a great source of motivation for me.

jonnyjames - July 30, 2025, 12:36 pm

One of the best OSINT THREAD I EVER SEEN thank u so much

DrunkProphet - July 30, 2025, 2:15 pm

This is such a good source of tools. Very on-point. Thanks. Almost like the osintframework for recon.

M2K - August 2, 2025, 2:55 am

Im slapping another comment on here to bump it up, this is such a great resource that should be pinned.

EUPHORIA - August 3, 2025, 4:52 pm

You should Add breachdirectory.org . Not bad for Passwords sometimes.

K4RM4 - August 3, 2025, 7:30 pm

Thank you for sharing! My ADHD is off the charts right now with all these new tools ?

??????????? - August 4, 2025, 1:55 am

(Aug 3, 2025 07:30 PM)Ab3Snak3 Wrote: [\[CITE\]](#) Thank you for sharing! My ADHD is off the charts right now with all these new tools ?

Glad to hear it.

passerino - August 12, 2025, 4:37 am

Thank you bro for sharing!

johndoeman805 - August 15, 2025, 4:34 pm

@??????? wow very informative thanks? however, very overwhelming due to all those choices. question: what are the best tools one would select for the job if they only had a twitter alias of the person of interest that one was trying to gather info on?

This is kinda like picking the right tools out of your toolbox on a construction site etc. ?

monikaindia - August 21, 2025, 9:09 am

good find

7 - August 21, 2025, 10:19 am

nice work ... paste the whole thread in claude and automate it.

passerino - August 21, 2025, 11:02 am

Thank you for sharing all these new tools

??????????? - August 21, 2025, 11:57 am

(Aug 21, 2025 11:02 AM)passerino Wrote: [\[CITE\]](#) Thank you for sharing all these new tools You are most welcome.

(Aug 21, 2025 10:19 AM)7 Wrote: [\[CITE\]](#) nice work ... paste the whole thread in claude and automate it.

Great idea.

ts1000 - August 21, 2025, 2:22 pm

Thanks <3

patchdev - September 4, 2025, 11:27 am

holy shit youre amazing

??????????? - September 4, 2025, 11:29 am

(Sep 4, 2025 11:27 AM)patchdev Wrote: [\[CITE\]](#) holy shit youre amazing Happy to see you find it useful.

DI?E - September 9, 2025, 9:30 pm

Nice and laid out well. I've known about a lot of these but its good to have them in a central place.
Good job.

psickophant - September 10, 2025, 5:32 pm

Well done! Thanks for sharing. I found it very helpful.

Gigabot - September 10, 2025, 7:02 pm

GQ post, thanks

cyborg24 - September 11, 2025, 8:34 am

Wow thank you! very comprehensive.

sadjasdjdsajdsad - September 13, 2025, 2:59 am

this was realler nice

orion11 - September 14, 2025, 7:17 am

Very nice thread. I love OSINT, so will def refer to this

???????????? - September 14, 2025, 11:45 am

(Sep 14, 2025 07:17 AM)orion11 Wrote: [\[CITE\]](#) Very nice thread. I love OSINT, so will def refer to this

Hope it helped?

MadScientist - September 17, 2025, 10:52 am

Great content as always!

???????????? - September 18, 2025, 5:44 am

(Sep 17, 2025 10:52 AM)MadScientist Wrote: [\[CITE\]](#) Great content as always!
Thanks for appreciating it. It inspires me to make more of these threads.

p89600 - September 20, 2025, 10:47 pm

Excellent resource. Many thanks.

Sergiarr - September 22, 2025, 9:48 am

one of the best thread i've seen huge thanks

???????????? - September 22, 2025, 9:49 am

(Sep 20, 2025 10:47 PM)p89600 Wrote: [\[CITE\]](#) Excellent resource. Many thanks.

(Sep 22, 2025 09:48 AM)Sergiarr Wrote: [\[CITE\]](#) one of the best thread i've seen huge thanks
Thankyou for checking it through.

oopsssnxgone - October 4, 2025, 9:07 am

WYo this the most viable osint package I've ever ran into

???????????? - October 18, 2025, 2:02 pm

(Oct 4, 2025 09:07 AM)oopsssnxgone Wrote: [\[CITE\]](#) WYo this the most viable osint package I've ever ran into

Glad it helped you with it.

Chorozon - October 30, 2025, 6:03 am

Good work OP solid guide

???????????? - October 31, 2025, 1:30 am

(Oct 30, 2025 06:03 AM)Chorozon Wrote: [\[CITE\]](#) Good work OP solid guide Thanks.

Tyr - November 17, 2025, 10:24 am

Killer guide and layout. W thread tbh.

Missing the GEOINT and HUMINT part though. ;)

???????????? - November 17, 2025, 10:26 am

(Nov 17, 2025 11:24 AM)Tyr Wrote: [\[CITE\]](#) Killer guide and layout. W thread tbh.

Missing the GEOINT and HUMINT part though. ;)
Thankyou. I will make another part of it adding them. :)

Tyr - November 17, 2025, 10:29 am

(Nov 17, 2025 11:26 AM)???????????? Wrote: [\[CITE\]](#) Thankyou. I will make another part of it adding them. :)

Was only teasing because you covered a ton of interrelated concepts in this thread but by all means, definitely do so when you have free time. I'd love to read up :)

???????????? - November 17, 2025, 10:37 am

(Nov 17, 2025 11:29 AM)Tyr Wrote: [\[CITE\]](#) Was only teasing because you covered a ton of interrelated concepts in this thread but by all means, definitely do so when you have free time. I'd love to read up :)

Appreciate it. I will mention you.

Orianna ? - November 19, 2025, 12:43 am

wow! basically made my cheat-sheet I did when I first started out. There is a lot of useful stuff here for beginners

VultureQuake - November 20, 2025, 4:37 am

huge thanks for such a great resource

???????????? - December 21, 2025, 11:44 am

(Nov 19, 2025 01:43 AM)Orianna ? Wrote: [\[CITE\]](#) wow! basically made my cheat-sheet I did when I first started out. There is a lot of useful stuff here for beginners
Beginners will find it very useful.

(Nov 20, 2025 05:37 AM)VultureQuake Wrote: [\[CITE\]](#) huge thanks for such a great resource

I am glad you liked it.

JollyHacka - December 28, 2025, 3:09 pm

Excellent post! A must have for any OSINT enthusiast.

bigcc - January 2, 2026, 2:17 pm

very good

BlackRock - January 3, 2026, 2:47 am

Thank you for compiling such a great amount of tools and resources.

???????????? - January 4, 2026, 8:05 am

(Jan 3, 2026 03:47 AM)BlackRock Wrote: [\[CITE\]](#) Thank you for compiling such a great amount of tools and resources.

Thanks for going through it.

6FOOT - January 5, 2026, 9:52 pm

Thanks alot , bout to build an ai agent

sdotarachj - January 6, 2026, 6:23 pm

Thank you! Commenting to save the post

M?tt - January 6, 2026, 6:45 pm

I'm surprised I never stumbled upon this earlier. Awesome thread.

???????????? - January 7, 2026, 8:30 am

(Jan 6, 2026 07:45 PM)M?tt Wrote: [\[CITE\]](#) I'm surprised I never stumbled upon this earlier. Awesome thread.

Thanks for appreciating.

SpiderSpicy - January 19, 2026, 2:56 pm

Nice amount of info together. This is one of the best explained thread that I have read so far.

tom45 - February 25, 2026, 2:48 am

thankas

CyberXero - September 9, 2026, 5:02 am

Damn this is definitely a gold mine!

Appreciate the effort you went through to provide this quality and quantity!

A lot of these have opened my eyes, enjoyed learning more then I knew even with the briefs of each tool in this OSINT and Recon toolkit

???????????? - September 9, 2026, 11:27 am

(Sep 9, 2026 05:02 AM)CyberXero Wrote: [\[CITE\]](#) Damn this is definitely a gold mine!

Appreciate the effort you went through to provide this quality and quantity!

A lot of these have opened my eyes, enjoyed learning more then I knew even with the briefs of each tool in this OSINT and Recon toolkit

Glad, you appreciated. ?

CyberXero - September 9, 2026, 11:32 am

(Sep 9, 2026 11:27 AM)???????????? Wrote: [\[CITE\]](#) Glad, you appreciated. ?

thanks for adding some value to my night, added it to the bookmarks!

I believe I will be using some of these tools real soon!

07days - September 9, 2026, 11:08 pm

Honestly, amazing amount of value for free. Appreciate it

Stanley - September 12, 2026, 6:19 am

I'm Stanley HF's helper bot. The OP (original poster) of this thread wants everyone to see this page and has elected to bump it to the top of the showthread listing. Since HF doesn't want a ton of LQP (Low Quality Posts) this is the best method of bumping your content. There is a small ?yte fee for each bump. Any OP can bump any of their threads on HF from the linked icon on the top of their first

post.

If you haven't already read the first post of this thread we encourage you to do so.

Thanks,
Stanley

SIGMA BOSS - *September 26, 2026, 10:39 pm*

Great thread

Uns77n - *September 27, 2026, 1:55 pm*

Thanks a lot for putting all that together