OSINT Investigator's Playbook

50+ Techniques to Find Anyone, Investigate Anything, and Uncover What's Hidden in Plain Sight

A Jimmy Tools Guide

jimmytools.net

Table of Contents

Chapter 1: Introduction to OSINT

Open Source Intelligence (OSINT) is the collection and analysis of information from publicly available sources. In an age where people voluntarily share vast amounts of personal information online, OSINT has become one of the most powerful investigative disciplines—used by journalists, law enforcement, intelligence agencies, corporate security teams, private investigators, and curious individuals.

This playbook will teach you the techniques professionals use to find people, investigate companies, verify identities, and uncover hidden connections. Everything described here uses legal, publicly available sources—no hacking, no unauthorized access, just the systematic exploitation of information people have made public.

What OSINT Can Reveal

- **Identity verification** – Confirm who someone really is
- **Location history** – Track where someone has lived, worked, or traveled
- **Relationships** – Map connections between people and organizations
- **Financial indicators** – Identify assets, business interests, lawsuits
- **Background details** – Criminal records, education, employment history
- **Online activity** – Social media posts, forum comments, dating profiles
- **Real estate** – Properties owned, values, mortgages, sales history
- **Corporate structures** – Business ownership, shell companies, connections

The OSINT Mindset

Effective OSINT isn't about knowing every tool—it's about systematic thinking:

1. **Define your objective** – What specifically do you want to learn?
2. **Identify selectors** – What data points do you have to start? (name, email, phone, photo)
3. **Map the data landscape** – Where might relevant information exist?
4. **Collect systematically** – Document everything, preserve evidence
5. **Analyze connections** – Look for patterns, corroborate findings
6. **Verify and validate** – Never trust a single source

> ⚠️ **Legal & Ethical Boundaries**
>
> OSINT uses only publicly available information. This guide does not cover hacking, unauthorized access, impersonation, or any illegal techniques. Even legal research can cross ethical lines—stalking, harassment, and doxing are never acceptable. Use these skills responsibly.

Chapter 2: Setting Up Your OSINT Workstation

Before diving into techniques, set up a proper research environment. A dedicated OSINT setup protects your privacy, keeps you organized, and makes investigations more efficient.

Browser Configuration

Use Separate Browser Profiles

- **Personal profile** – Your regular browsing, logged into your accounts
- **OSINT profile** – Clean profile, no logins, private browsing
- **Sock puppet profile** – For research accounts (see OPSEC chapter)

Essential Browser Extensions

Extension	Purpose
uBlock Origin	Ad/tracker blocking
Privacy Badger	Tracker detection
Wayback Machine	Quick access to archived pages
Exif Viewer	View image metadata
User-Agent Switcher	Spoof browser identity
DownThemAll	Bulk downloads
SingleFile	Save complete webpages

VPN & Anonymity

A VPN hides your IP address from sites you visit—essential when researching subjects who might monitor for investigators. Choose a reputable no-logs VPN like Mullvad, ProtonVPN, or IVPN.

For higher-risk investigations, consider using Tor Browser, which routes traffic through multiple relays. However, many sites block Tor exit nodes.

Documentation Tools

- **Hunchly** – Automatic web capture and case management (paid, excellent)
- **Obsidian** – Note-taking with linking for relationship mapping
- **Maltego** – Visual link analysis (free community edition)
- **Archive-It / HTTrack** – Website archiving
- **Spreadsheets** – Simple but effective for tracking data points

> 💡 **The Sock Puppet Kit**
>
> For social media research, you'll need "sock puppet" accounts—fake personas not connected to your real identity. Create accounts with burner email addresses, VPN, and stock photos (properly licensed). Keep detailed notes on each persona. Chapter 18 covers this in depth.

Chapter 3: Search Engine Mastery

Google is powerful, but most people only scratch the surface. Advanced search operators let you find specific content that basic searches miss.

Essential Google Operators

Operator	Function	Example
`"exact phrase"`	Exact match	`"john smith" dallas`
`site:`	Search specific site	`site:linkedin.com "john smith"`
`-keyword`	Exclude term	`"john smith" -facebook`
`filetype:`	Specific file type	`filetype:pdf budget 2024`
`inurl:`	Term in URL	`inurl:admin login`
`intitle:`	Term in page title	`intitle:"index of" passwords`
`intext:`	Term in page body	`intext:"confidential"`
`before:` / `after:`	Date range	`after:2023-01-01 before:2024-01-01`
`cache:`	Cached version	`cache:example.com`
`related:`	Similar sites	`related:nytimes.com`

Google Dorking: Finding Exposed Data

"Google dorks" are search queries that find exposed files, directories, and sensitive data. Examples:

- `filetype:xls "password"` – Excel files containing passwords
- `intitle:"index of" "backup"` – Open directory listings with backups
- `site:pastebin.com "company name"` – Leaked data on paste sites
- `inurl:wp-content/uploads filetype:pdf` – PDF uploads on WordPress sites

- `"email" "phone" filetype:csv` – Contact lists in CSV format

> 🔧 **Google Dork Resources**
>
> - **Google Hacking Database (GHDB)** – Exploit-DB's collection of dorks
> - **DorkSearch** – Pre-built dork generator
> - **Pentest-Tools Google Dorks** – Curated security-focused dorks

Alternative Search Engines

Different engines index different content. Cross-reference results:

- **Bing** – Different algorithm, sometimes finds things Google misses
- **DuckDuckGo** – Privacy-focused, uses Bing index
- **Yandex** – Russian engine, excellent for facial recognition image search
- **Baidu** – Chinese content and Asian websites
- **Brave Search** – Independent index
- **Ahmia** – Tor hidden services search

People-Specific Search Engines

Site	Best For
Pipl.com (paid)	Deep identity search, email/phone lookup
ThatsThem.com	Free people search, addresses, phones
FastPeopleSearch.com	Free comprehensive people search
TruePeopleSearch.com	Free, good for current addresses
Spokeo.com (paid)	Social media aggregation
BeenVerified (paid)	Background check style reports

Chapter 4: Social Media Intelligence

Social media is the richest source of personal information. People reveal their locations, relationships, employers, daily routines, and opinions—often without realizing the investigative gold they're providing.

Facebook Investigation

Profile Discovery

- Search by name + location, employer, or school
- Use Graph Search alternatives: Social Searcher, StalkFace
- Find Facebook ID: View page source, search for "entity_id"
- Direct URL: facebook.com/[username] or facebook.com/profile.php?id=[ID]

Extracting Information

- **Friends list** – Reveals relationships even if hidden (via mutual friends)
- **Tagged photos** – Shows connections and locations
- **Check-ins** – Historical location data
- **Likes/Groups** – Interests, affiliations, communities
- **Life events** – Jobs, education, relationships with dates

Facebook-Specific Tools

- **Who Posted What** (whopostedwhat.com) – Search Facebook posts by keyword/date
- **Lookup-ID** (lookup-id.com) – Find Facebook ID from URL
- **IntelligenceX Facebook Search** – Historical data

Instagram Investigation

- **Username search** – instagram.com/[username]
- **Location tags** – Click location to see all posts at that spot
- **Hashtag research** – Find related posts and accounts

- **Story highlights** – Often contain older revealing content
- **Tagged photos** – Check what others post about them

> 🔧 **Instagram Tools**
>
> - **ImgInn** – View stories anonymously
> - **StoriesIG** – Download stories
> - **Dumpor** – Profile viewer without login
> - **Picuki** – Browse and download content

Twitter/X Investigation

- **Advanced Search** – twitter.com/search-advanced (dates, accounts, keywords)
- **From:username** – All tweets from specific account
- **To:username** – Replies to someone
- **@username filter:media** – Only media posts
- **geocode:lat,long,radius** – Tweets from specific location

Twitter Search Operators

```
"exact phrase" from:username since:2023-01-01 until:2024-01-01 -filter:retweets
```

LinkedIn Investigation

LinkedIn reveals professional history, connections, and organizational structures.

- **Google dorking** – `site:linkedin.com/in "john smith" dallas`
- **Company pages** – See all employees, org chart
- **Alumni search** – Find people by school and graduation year
- **Connections** – Map professional networks
- **Activity** – Posts, comments, likes reveal interests

> ⚠️ **LinkedIn Shows Who Viewed**
>
> LinkedIn notifies users when someone views their profile (unless you use LinkedIn Premium's private mode). Use logged-out searching, Google cache, or IntelligenceX to avoid detection.

TikTok, Snapchat, Discord

- **TikTok** – Search by username, hashtag, sounds. Videos often reveal location/lifestyle
- **Snapchat Map** – Public snaps appear on map with location
- **Discord** – Server search tools, user ID lookup, bot-based searching

Username Correlation

People reuse usernames across platforms. Find all accounts linked to one username:

Tool	URL
Namechk	namechk.com
WhatsMyName	whatsmyname.app
KnowEm	knowem.com
Sherlock	GitHub (command line)
Maigret	GitHub (advanced Sherlock fork)

Chapter 5: People Search & Identification

Finding and identifying people is core to OSINT. This chapter covers techniques for locating individuals, verifying identities, and mapping their digital footprint.

Starting with a Name

1. **Google the name** (with quotes) + location, employer, or other identifier
2. **Check people search sites** – FastPeopleSearch, ThatsThem, TruePeopleSearch
3. **Search social media** – Facebook, LinkedIn, Instagram, Twitter
4. **Check voter records** – Many states publish voter files with addresses, DOB
5. **Property records** – County assessor sites show ownership
6. **Court records** – Civil and criminal cases

Starting with an Email Address

1. **Google the email** – May appear in leaked databases, forum posts, documents
2. **Check Have I Been Pwned** – Shows data breaches containing the email
3. **Email to social** – Epieos, Holehe check which platforms have accounts
4. **Domain whois** – If custom domain, check registration info
5. **Gravatar** – gravatar.com/[md5 hash of email] may show photo

> 🔧 **Email Investigation Tools**
>
> - **Epieos** – Email to social media accounts
> - **Holehe** – Check email registration on 120+ sites
> - **Hunter.io** – Find corporate email patterns
> - **EmailRep** – Reputation and associations
> - **Have I Been Pwned** – Breach database search

Starting with a Phone Number

1. **Reverse phone lookup** – TruePeopleSearch, ThatsThem, Whitepages
2. **Google the number** – May appear in ads, posts, business listings
3. **Check caller ID apps** – Truecaller, Hiya (may show saved name)
4. **Carrier lookup** – Identify carrier and number type (mobile/landline/VoIP)
5. **WhatsApp/Telegram** – Add number to see profile photo/name

Starting with a Photo

Reverse image search finds where a photo appears online and can identify people:

Service	Strength
Google Images	General reverse search
Yandex Images	Best for facial recognition
TinEye	Finding image origins and modifications
PimEyes (paid)	Facial recognition across web
FaceCheck.ID	Face matching

> 💡 **Yandex is Underrated**
>
> Yandex's image search has remarkably good facial recognition. It often identifies people that Google Images misses. Always include Yandex in your reverse image workflow.

Identity Verification Techniques

Once you find information, verify it's the right person:

- **Cross-reference multiple sources** – Same info from 3+ sources = higher confidence
- **Check for unique identifiers** – Middle name, exact DOB, relatives' names
- **Timeline consistency** – Do job dates, addresses, ages align?
- **Photo matching** – Compare photos across platforms

- **Writing style** — Language patterns consistent across accounts?

Chapter 6: Business & Corporate Research

Corporate OSINT reveals company structures, ownership, financial health, and hidden connections. Whether investigating a business partner, competitor, or suspicious entity, these techniques expose what companies want hidden.

State Business Registrations

Every business entity (LLC, Corporation, etc.) must register with a state. These records reveal:

- Date of formation
- Registered agent (receives legal notices)
- Officers and directors
- Business address
- Annual filings and status

Key Resources

Source	Coverage
OpenCorporates	200M+ companies worldwide
State SOS websites	Official state records (search "[state] secretary of state business search")
Cobalt Intelligence	Multi-state aggregated search
Corporation Wiki	Free company/officer search

SEC Filings (Public Companies)

Public companies must file detailed reports with the SEC. Key filings:

- **10-K** – Annual report (comprehensive business overview)
- **10-Q** – Quarterly financial reports
- **8-K** – Material events (mergers, lawsuits, executive changes)
- **DEF 14A** – Proxy statement (executive compensation, shareholders)

- **Form 4** – Insider trading reports
- **Schedule 13D/G** – Large shareholder disclosures

Search at: **sec.gov/edgar/searchedgar/companysearch.html**

Uncovering Shell Companies

Shell companies hide ownership. Red flags:

- Registered agent services (CT Corporation, CSC, Registered Agent Inc.)
- Formation in Delaware, Wyoming, Nevada (strong privacy laws)
- No physical office or employees
- Officers are other companies or nominees
- Recent formation with large asset purchases

Piercing the Corporate Veil

1. Check registered agent—same agent = possibly same owner
2. Search officer names across states
3. Look for common addresses across entities
4. Check UCC filings for financing relationships
5. Search real property records for corporate ownership

Government Contracts & Grants

Source	What It Shows
USAspending.gov	All federal spending, contracts, grants
FPDS.gov	Federal procurement data
SAM.gov	Contractor registrations and exclusions
Grants.gov	Grant opportunities and awards
GovTribe	Contract analysis and intelligence

Offshore & International Companies

- **ICIJ Offshore Leaks Database** – Panama Papers, Pandora Papers data
- **OpenCorporates** – Global company search
- **UK Companies House** – Excellent free data on UK companies
- **GLEIF** – Legal Entity Identifier database

Chapter 7: Property & Asset Discovery

Real property records are public in the United States, making property ownership one of the easiest assets to research. This chapter covers techniques for finding who owns what.

Real Property Records

County Assessor/Recorder Offices

Every county maintains property records showing:

- Current owner name
- Mailing address (sometimes different from property)
- Assessed value and taxes
- Property characteristics (size, beds/baths, year built)
- Sales history and prices
- Mortgage information

Free Property Search Sites

Site	Coverage
Zillow	National, estimates and history
Redfin	National, detailed records
County assessor websites	Official records
NETR Online	Links to county record sites
SearchSystems.net	Public record database directory

Finding Hidden Ownership

Properties may be held in LLCs, trusts, or corporate names. To find the real owner:

1. Note the LLC/trust name on the deed

2. Search state business records for LLC officers
3. Check if the LLC's registered agent address matches other properties
4. Search the trust name in court records (trusts often appear in probate)
5. Look for financing documents—lenders often require personal guarantees

Vehicle Records

Vehicle ownership is harder to research due to DPPA restrictions, but some avenues exist:

- **VIN lookup** – NICB VinCheck (theft/total loss), NHTSA recalls
- **License plate lookup** – Limited legal options for non-law enforcement
- **Parking/traffic tickets** – Sometimes appear in court records
- **Social media** – People post their vehicles
- **Business vehicles** – DOT numbers, fleet registrations

Aircraft & Boats

Aircraft and boat registrations are more accessible:

Asset	Source
Aircraft	FAA Registry (registry.faa.gov)
Boats (documented)	USCG NVDC (st.nmfs.noaa.gov/st1/CoastGuard/)
Boats (state)	State DMV/wildlife agency
Flight tracking	FlightAware, ADS-B Exchange
Ship tracking	MarineTraffic, VesselFinder

UCC Filings

Uniform Commercial Code filings record security interests in personal property. When someone takes a loan secured by equipment, inventory, or accounts receivable, a UCC-1 is filed. These reveal:

- Debtor name and address
- Secured party (lender)

- Collateral description
- Filing date and status

Search at state SOS websites or aggregators like BizFilings.

Chapter 8: Domain & Website Investigation

Every website leaves a trail. Domain registration, hosting, historical content, and technical details can reveal who's behind a site and how it's connected to others.

WHOIS Lookup

Domain registration records often show owner information (though privacy services are common):

- **ICANN WHOIS** – lookup.icann.org
- **DomainTools** – Comprehensive WHOIS history (paid)
- **WhoisXML API** – Historical and reverse WHOIS
- **ViewDNS.info** – Multiple DNS tools

Key WHOIS Fields

- **Registrant** – Domain owner (may be privacy-protected)
- **Creation date** – When domain was first registered
- **Name servers** – Can link related domains
- **Registrar** – Where domain was purchased

Historical WHOIS

Even if current WHOIS is private, historical records may show previous owners:

- **DomainTools WHOIS History**
- **WhoisXML Historical WHOIS**
- **SecurityTrails**

Reverse IP & DNS

Find other sites on the same server or with related infrastructure:

Tool	Function

ViewDNS Reverse IP	Sites sharing IP address
SecurityTrails	DNS history and associations
Shodan	Internet-connected device search
Censys	Certificate and host search
DNSDumpster	DNS reconnaissance

Website Archives

The Wayback Machine (web.archive.org) stores historical snapshots of websites. Use it to:

- See how a site looked in the past
- Recover deleted content
- Find old contact information, team pages, etc.
- Document changes over time

SSL Certificate Analysis

SSL certificates can reveal related domains and organization info:

- **crt.sh** – Certificate transparency logs
- **Censys Certificates** – Search by organization, domain

Technology Fingerprinting

Identify what technology a site uses:

- **BuiltWith** – Technology stack analysis
- **Wappalyzer** – Browser extension for tech detection
- **WhatRuns** – Similar to BuiltWith

Chapter 9: Email Intelligence

Email addresses are valuable selectors for investigation. This chapter covers techniques for extracting maximum intelligence from an email address.

Email Validation

First, verify the email exists:

- **Hunter.io Email Verifier**
- **NeverBounce**
- **ZeroBounce**

Email to Identity

Check Social Platforms

- **Epieos** – Checks Google, Skype, and more
- **Holehe** – Checks 120+ platforms
- **GHunt** – Google account investigation (GitHub tool)

Gravatar & Avatar Services

Many sites use Gravatar for profile photos. Check: `gravatar.com/avatar/[MD5 hash of email]`

Breach Data

Email addresses appear in data breaches. Legitimate services to check:

- **Have I Been Pwned** – haveibeenpwned.com
- **DeHashed** – Breach database search
- **IntelligenceX** – Includes some breach data

> ⚠️ **Legal Warning**
>
> Accessing or using stolen credentials is illegal. Breach data services are useful for seeing which breaches an email appeared in, but don't access actual leaked passwords or use them.

Corporate Email Patterns

If you know someone works at a company but not their email:

1. Find the company's email pattern (john.smith@, jsmith@, john_smith@)
2. Construct the likely email
3. Verify it exists

Hunter.io and **RocketReach** help identify corporate email patterns.

Chapter 10: Phone Number Research

Carrier Identification

Determine if a number is mobile, landline, or VoIP:

- **Twilio Lookup API**
- **NumVerify**
- **Carrier Lookup tools**

Reverse Phone Lookup

Service	Type
TruePeopleSearch	Free
ThatsThem	Free
Whitepages	Freemium
Spy Dialer	Free voicemail lookup
Truecaller	App-based caller ID

Phone to Social Media

- **Facebook** – Search by phone number (if not privacy-protected)
- **WhatsApp** – Add number to contacts, see profile photo/status
- **Telegram** – Search by phone number
- **Signal** – Will show if number is registered
- **Viber** – Shows name if user has account

Google the Number

Search the number (with and without dashes/spaces) to find:

- Classified ads
- Business listings
- Social media posts
- Spam reports
- Forum posts

Chapter 11: Image & Video Analysis

Reverse Image Search

Always use multiple engines:

1. **Google Images** – General search
2. **Yandex** – Best facial recognition
3. **TinEye** – Finding original and modifications
4. **Bing Visual Search** – Alternative results

EXIF Data Extraction

Photos contain metadata (EXIF) that may include:

- Camera make/model
- Date and time taken
- GPS coordinates (!)
- Software used to edit

Tools: Jeffrey's EXIF Viewer, FotoForensics, ExifTool

> 💡 **EXIF Often Stripped**
>
> Most social media platforms strip EXIF data on upload. However, photos sent via email, posted on forums, or downloaded from cloud storage often retain it.

Image Forensics

Detect manipulated images:

- **FotoForensics** – Error level analysis
- **InVID/WeVerify** – Video/image verification toolkit
- **Forensically** – Browser-based image forensics

Facial Recognition

Service	Notes
Yandex Images	Free, effective
PimEyes	Paid, powerful but controversial
FaceCheck.ID	Face search across web

Chapter 12: Geolocation Techniques

Geolocation—determining where a photo or video was taken—is one of OSINT's most powerful techniques. Combine visual clues with mapping tools to pinpoint locations.

Visual Clues to Look For

- **Signs and text** – Street signs, business names, license plates
- **Architecture** – Building styles vary by region
- **Vegetation** – Plants indicate climate/region
- **Sun position** – Indicates hemisphere and time
- **Shadows** – Help determine time of day
- **Infrastructure** – Power lines, road markings, vehicle types
- **Landmarks** – Mountains, towers, distinctive buildings

Geolocation Tools

Tool	Use
Google Maps/Earth	Street View, satellite imagery
Google Earth Pro	Historical imagery, measurements
SunCalc	Sun position calculator
ShadowCalculator	Shadow analysis
GeoSpy	AI-based location estimation
What3Words	Precise location encoding

The Geolocation Process

1. **Identify all visible clues** in the image
2. **Research clues** – What do signs say? What language?

3. **Narrow to region** – Country, then city/area
4. **Search Street View** for matching location
5. **Verify** – Do all clues align?

Chapter 13: Vehicle & Transportation

Flight Tracking

- **FlightAware** – Flight tracking, historical data
- **FlightRadar24** – Real-time global flight tracking
- **ADS-B Exchange** – Unfiltered ADS-B data (no blocked aircraft)
- **FAA Registry** – Aircraft ownership records

Ship Tracking

- **MarineTraffic** – Vessel positions and history
- **VesselFinder** – Ship tracking
- **MyShipTracking** – Free vessel tracking

Vehicle Identification

- **VIN decoding** – NHTSA VIN decoder, VinDecoder.net
- **License plate lookup** – Limited without law enforcement access
- **Parking ticket databases** – Some cities publish online

Chapter 14: Financial Research

SEC Filings

EDGAR (sec.gov/edgar) contains all public company filings. Key searches:

- Company filings by name/ticker
- Full-text search across all filings
- Insider trading (Form 4)
- 13F institutional holdings

Campaign Finance

- **FEC.gov** – Federal campaign contributions
- **OpenSecrets** – Campaign finance analysis
- **FollowTheMoney** – State-level contributions

Lobbying Records

- **Senate Lobbying Disclosures**
- **House Lobbying Disclosures**
- **OpenSecrets Lobbying**
- **FARA** – Foreign agent registrations

Bankruptcy & Liens

- **PACER** – Federal bankruptcy court records
- **State UCC filings** – Security interests
- **Tax liens** – County recorder offices

Chapter 15: Court Records & Legal Research

Federal Courts (PACER)

PACER (pacer.uscourts.gov) contains federal court records:

- Civil cases
- Criminal cases
- Bankruptcy
- Appeals

Costs $0.10/page, but first $30/quarter is free. **RECAP** browser extension provides free access to previously-downloaded documents.

State Courts

Each state has its own system. Many offer free online search:

- Search "[state] court case search"
- Check both state and county court systems
- Criminal, civil, family, and probate courts may be separate

Legal Research

- **Google Scholar** – Free case law search
- **CourtListener** – Free legal database
- **Justia** – Free legal information
- **CaseText** – Case law with AI features

Chapter 16: Dark Web Basics

The dark web contains hidden services not indexed by regular search engines. While often associated with illegal activity, it also hosts legitimate privacy-focused services and can be useful for OSINT.

Accessing the Dark Web

1. Download **Tor Browser** from torproject.org
2. Connect to Tor network
3. Access .onion addresses

> ⚠️ **Proceed with Caution**
>
> The dark web contains illegal content including marketplaces for drugs, weapons, and stolen data. Viewing such content may be illegal. Use Tor only for legitimate research purposes.

Dark Web Search Engines

- **Ahmia** – ahmia.fi (clearnet) or ahmia.onion
- **DuckDuckGo** – duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswzczad.onion
- **Torch** – Dark web search engine

Legitimate Dark Web Research Uses

- Monitoring for leaked credentials
- Researching threat actors
- Accessing privacy-focused services
- Journalism source protection

Chapter 17: Archiving & Preservation

Online content disappears. Preserve evidence before it's deleted.

Why Archive?

- Content gets deleted or edited
- Websites go offline
- Evidence may be needed for legal proceedings
- Historical documentation

Archiving Tools

Tool	Use
Wayback Machine	Submit URLs for archiving
Archive.today	Quick page snapshots
Hunchly	Automatic capture during browsing
SingleFile	Save complete pages as single HTML
HTTrack	Download entire websites
youtube-dl	Download videos

Chain of Custody

For evidence that may be used in legal proceedings:

- Document exactly when and how you captured it
- Use tools that create timestamps and hashes
- Store originals separately from working copies
- Consider notarized screenshots for critical evidence

Chapter 18: OPSEC: Protecting Yourself

When investigating, protect your own identity and digital footprint.

Browser Separation

- Use separate browser profiles for research
- Never log into personal accounts while researching
- Consider a dedicated research VM

VPN & Anonymity

- Use VPN for all research
- Tor for sensitive investigations
- Rotate exit nodes/servers

Sock Puppet Accounts

Create research personas:

- Use burner email (ProtonMail, Tutanota)
- VPN/Tor when creating
- Consistent but fictional persona
- Profile photos from ThisPersonDoesNotExist.com or properly licensed stock
- Build history before using for research

> ⚠️ **Account Policies**
>
> Creating fake accounts violates most platforms' terms of service. While common in OSINT, be aware of the risks and never use fake accounts for illegal purposes.

Physical Security

For sensitive investigations:

- Don't research from identifiable locations
- Be aware of who can see your screen
- Use encrypted storage for research files
- Consider the legal implications of your investigation

Chapter 19: Case Study Walkthroughs

Case 1: Finding a Person with Only a Name

Scenario: Find "Michael Johnson" who works in tech in Austin, TX.

1. Google: `"Michael Johnson" Austin tech`
2. LinkedIn: `site:linkedin.com "michael johnson" austin`
3. Narrow by employer, school, or other identifier
4. Cross-reference social media (Facebook, Twitter)
5. Check voter records (many states publish)
6. Property records in Travis County
7. Verify by matching photos, timeline, connections

Case 2: Investigating a Suspicious Company

Scenario: ABC Consulting LLC solicits your business. Verify legitimacy.

1. State business registration – when formed, who are officers?
2. WHOIS on their domain – when registered, by whom?
3. LinkedIn company page – do employees look real?
4. Google reviews, BBB, Glassdoor
5. Reverse image search any photos
6. Check if address is a virtual office
7. Search officer names for other businesses, lawsuits

Case 3: Verifying a Social Media Profile

Scenario: Someone claims to be a doctor. Verify.

1. Check medical license databases (state medical board)
2. NPI (National Provider Identifier) registry
3. Hospital/practice affiliation verification

4. Medical school alumni directories
5. Cross-reference photo with other sources
6. Check for disciplinary actions

Chapter 20: Tool Reference & Resources

Essential Bookmarks

Search

- Google Advanced Search
- Yandex Images
- IntelligenceX

People

- FastPeopleSearch
- ThatsThem
- TruePeopleSearch
- Pipl (paid)

Social Media

- Namechk (username search)
- Sherlock/Maigret (command line)
- Social Searcher

Email

- Hunter.io
- Epieos
- Have I Been Pwned

Business

- OpenCorporates
- SEC EDGAR
- State SOS websites

Property

- County assessor sites
- Zillow/Redfin
- FAA Registry

Web/Domain

- WHOIS lookup
- Wayback Machine
- SecurityTrails
- Shodan

Comprehensive Tool Collections

- **OSINT Framework** – osintframework.com
- **Bellingcat Online Investigation Toolkit**
- **IntelTechniques** – inteltechniques.com
- **Awesome OSINT** – GitHub repository

Learning Resources

- **Bellingcat** – bellingcat.com (case studies)
- **SANS OSINT courses**
- **Trace Labs** – Missing persons OSINT CTF
- **r/OSINT** – Reddit community

About Jimmy Tools

Jimmy Tools provides research guides, databases, and analysis tools for investigators, journalists, and curious citizens. Our mission is to make powerful research capabilities accessible to everyone.

Visit us at **jimmytools.net**