OSINT Experimentation Suite

8 Tools + Extended Techniques for Six Degrees Identity Investigation

Objective	Prove Six Degrees of Separation through practical OSINT experimentation
Method	Username permutation → platform sweep → graph expansion → Bayesian scoring
Target context	Chilean social network users (Facebook, Instagram, WhatsApp, Twitter/X)
Math basis	Milgram 1967, Watts-Strogatz 1998, Bayes theorem, BFS graph traversal
OS	Ubuntu 22.04 / Debian — all tools open source

1. Experiment Overview & Theoretical Foundation

The experiment is structured as a layered pipeline. Each tool corresponds to a specific phase of the investigation and a specific degree in the Six Degrees model. The goal is to start from a name only (minimum viable input) and progressively build a social graph around the target.

Pipeline at a glance:

Phase	Degree	Goal	Tool(s)
1 — Seed	0	Generate username candidates from real name	Username Anarchy
2 — Sweep	0	Detect active profiles on 400+ platforms	Sherlock, Maigret
3 — Deep cluster	0-1	Link profiles across platforms, build identity graph	Maigret, SpiderFoot
4 — Email pivot	0	Confirm identity via email address	Holehe
5 — Name search	0	Real-name search for non-technical users	Google Dorks
6 — Social graph	1	Access direct connections (friends, followers)	Facebook Search
7 — Phone pivot	0	Verify WhatsApp presence via phone number	WhatsApp wa.me
8 — Graph expand	1-3	Automated BFS expansion of the social graph	SpiderFoot
9 — Scoring	all	Bayesian confidence per profile found	Custom scorer
10 — Extra tech.	all	Reverse image, EXIF, metadata, TikTok, LinkedIn	Various

2. The 8 Tools — Commands & Experimental Purpose

Tool 1 — Username Anarchy | Seed Generation (Degree 0)

Username Anarchy generates all statistically probable username permutations from a first and last name. It applies linguistic rules (initials, concatenation, separators, leet substitutions) producing 50-200 candidates. This seed list is the input for all subsequent tools. Without good seeds, the sweep phase misses profiles.

Install:

```
sudo apt install ruby -y git clone https://github.com/urbanadventurer/username-anarchy ~/osint-tools/username-anarchy
```

Best experimental command:

```
ruby ~/osint-tools/username-anarchy/username-anarchy.rb Francisco Munoz > usernames.txt # Chile-specific additions: echo 'francisco_cl' >> usernames.txt echo 'el_francisco' >> usernames.txt echo 'fjmunoz' >> usernames.txt sort -u usernames.txt -o usernames.txt wc -l usernames.txt # verify count
```

Experiment note: Run for both apellido paterno and apellido materno separately. Also run without accents/ñ — Chilean users almost always register as 'Munoz' not 'Muñoz'.

Tool 2 — Sherlock | Fast Platform Sweep (Degree 0)

Sherlock queries 400+ websites simultaneously checking if a username exists. It is optimized for speed and breadth. The best experimental approach is to run the top 5 most probable usernames and filter results to Chile-relevant platforms. Sherlock proves or disproves Degree 0 presence.

Install:

```
pip3 install sherlock-project
```

Best experimental commands:

```
# Sweep top usernames, save only found profiles sherlock franciscomunoz fjmunoz fmunoz francisco_munoz javimunoz \ --print-found --timeout 10 --output results_sherlock.txt # Filter Chile-relevant platforms from results grep -iE 'instagram|facebook|twitter|tiktok|linkedin|pinterest' results_sherlock.txt # Single site verification (fast confirmation) sherlock franciscomunoz --site instagram --print-found sherlock franciscomunoz --site twitter --print-found
```

Experiment note: Sherlock returns false positives on some platforms. Always manually verify each [+] result by visiting the URL before scoring it.

Tool 3 — Maigret | Identity Clustering & Graph (Degree 0-1)

Maigret goes beyond Sherlock by analyzing tags and cross-references between found profiles. It detects when one profile mentions another platform (e.g., an Instagram bio linking to Twitter), building an identity cluster that constitutes the beginning of the Degree 1 graph. It also generates PDF/HTML reports automatically.

Install:

```
pip3 install maigret
```

Best experimental commands:

```
# Full scan with PDF + HTML report and social tag filter maigret franciscomunoz \
--folderoutput ./maigret_results \ --report pdf \ --report html \ --tags social \
--no-progressbar # Run multiple usernames from the seed list (batch) while read -r user;
do maigret "$user" --folderoutput ./maigret_results --no-progressbar 2>/dev/null done <
usernames.txt # View generated reports ls ./maigret_results/
```

Experiment note: Maigret's identity graph in the HTML report visually shows connections between profiles — this directly illustrates the Degree 0 to Degree 1 transition in the Six Degrees model.

Tool 4 — Holehe | Email Pivot (Degree 0 Confirmation)

Holehe checks whether an email address is registered on 120+ platforms. If the target's email is known (or can be guessed from common patterns), Holehe rapidly confirms which services they use — providing strong Bayesian evidence for identity confirmation.

Install:

```
pip3 install holehe
```

Best experimental commands:

```
# Check a known email, show only platforms where account exists holehe
francisco.munoz@gmail.com --only-used # Test multiple probable email patterns (Chilean
common formats) for email in \ francisco.munoz@gmail.com \ franciscomunoz@gmail.com \
f.munoz@gmail.com \ francisco.munoz@hotmail.com; do echo "--- Testing: $email ---"
holehe "$email" --only-used 2>/dev/null done # Save results to file holehe
francisco.munoz@gmail.com --only-used > holehe_results.txt
```

Experiment note: Common Chilean email patterns are firstname.lastname@gmail.com and firstnamelastname@hotmail.com. Hotmail/Outlook is still widely used by older demographics in Chile.

Tool 5 — Google Dorks | Real Name Search (Degree 0)

Google Dorks are advanced search operators that restrict results to specific sites or formats. For non-technical users who use their real name on social media (very common in Chile on Facebook), dorks are often more effective than username-based tools because they search the actual name, not a handle.

Best experimental dorks:

```
# Degree 0 — Direct profile search by real name site:instagram.com "Francisco Munoz"
site:facebook.com "Francisco Munoz" site:twitter.com "Francisco Munoz"
site:linkedin.com "Francisco Munoz" site:tiktok.com "Francisco Munoz" # Degree 0 —
Narrow to Chile "Francisco Munoz" Chile "Francisco Munoz" Santiago "Francisco Munoz"
"@gmail.com" OR "@hotmail.com" # Degree 1 — Find who mentions the target (indirect
connections) "Francisco Munoz" -site:instagram.com -site:facebook.com # Cross-platform
correlation "Francisco Munoz" site:instagram.com OR site:twitter.com OR site:tiktok.com
# Find cached/deleted profiles cache:instagram.com/franciscomunoz
```

Experiment note: The minus operator (-site:) is key to finding Degree 1 mentions — people who tag or write about the target on platforms outside their own profiles.

Tool 6 — Facebook People Search | Degree 1 Graph Access

Facebook's internal search is the most powerful tool for Chilean investigations because the majority of non-technical Chilean users maintain real-name Facebook profiles. The People Search directly exposes the Degree 1 graph (friends, family, coworkers) when profiles are public or semi-public.

Best experimental URLs (open in browser):

```
# People search — returns profiles matching the name
https://www.facebook.com/search/people/?q=Francisco%20Munoz # Posts mentioning the name
```

```
— reveals Degree 1 (who talks about target)
https://www.facebook.com/search/posts/?q=Francisco%20Munoz # Photos tagged with the
name https://www.facebook.com/search/photos/?q=Francisco%20Munoz # Groups the target
might belong to https://www.facebook.com/search/groups/?q=Francisco%20Munoz # Events —
reveals location patterns and associates
https://www.facebook.com/search/events/?q=Francisco%20Munoz
```

Experiment note: Once a profile is found, examine 'Friends' (if public), tagged photos, and comments on posts. Each commenter is a Degree 1 node. Repeat the Bayesian scoring for each connection found to build the graph.

Tool 7 — WhatsApp Phone Verification | Phone Pivot (Degree 0)

WhatsApp is the primary communication platform in Chile with over 85% penetration. If a phone number is known (from a public listing, business card, or other source), the wa.me link test quickly confirms whether the number is active on WhatsApp. WhatsApp profile photos and status messages are often publicly visible.

Best experimental commands:

```
# Test if number is active on WhatsApp (HTTP 200 = active) curl -s -o /dev/null -w
'%{http_code}' --max-time 10 https://wa.me/56912345678 # Open directly in browser to see
profile photo + status # https://wa.me/56912345678 # Check multiple numbers in batch for
number in 56912345678 56987654321 56911223344; do STATUS=$(curl -s -o /dev/null -w
'%{http_code}' --max-time 8 "https://wa.me/$number") echo "$number → HTTP $STATUS" done
# Chilean mobile number format: 569XXXXXXXX # (56 = country code, 9 = mobile prefix,
XXXXXXXX = 8 digits)
```

Experiment note: HTTP 200 does not guarantee the number belongs to the target — it only confirms the number is registered on WhatsApp. Always cross-reference the profile photo with other platforms using reverse image search.

Tool 8 — SpiderFoot | Automated Six Degrees Graph Expansion (Degree 1-3)

SpiderFoot is the most academically aligned tool in the suite. It implements automated BFS-style graph expansion, following links and associations from the seed target outward. It correlates data across 200+ data sources and visualizes the resulting graph — directly proving the Six Degrees theory by showing the chain of connections.

Install:

```
pip3 install spiderfoot --break-system-packages
```

Best experimental commands:

```
# Start web UI (recommended — includes graph visualization) python3 -m spiderfoot -l
127.0.0.1:5001 # Then open http://127.0.0.1:5001 in browser # New scan → target:
'Francisco Munoz' → type: Human Name # Enable modules: sfp_social, sfp_account,
sfp_webanalytics, sfp_names # CLI mode — output as table python3 -m spiderfoot -s
"Francisco Munoz" -t HUMAN_NAME \ -m sfp_social,sfp_account,sfp_names \ -o table
2>/dev/null # CLI mode — output as JSON for further processing python3 -m spiderfoot -s
"Francisco Munoz" -t HUMAN_NAME \ -m sfp_social,sfp_account,sfp_names \ -o json
2>/dev/null > spiderfoot_results.json
```

Experiment note: SpiderFoot's graph view in the web UI visually demonstrates the Six Degrees model — each node is a person or profile, each edge is a connection. Count the hops from target to any other node to empirically measure degrees of separation.

3. Extended Techniques

Beyond the 8 core tools, the following techniques significantly enhance the investigation and provide additional evidence signals for the Bayesian scoring model.

3.1 Reverse Image Search | Cross-Platform Visual Confirmation

When a profile photo is found, reverse image search can locate the same photo on other platforms, confirming the same person uses multiple accounts. This is one of the strongest confirmation signals and adds +0.20 to the Bayesian score.

```
# Download profile photo first curl -o profile.jpg
'https://instagram.com/...profile_pic_url...' # Reverse image search URLs (open in
browser) # Google Images: https://images.google.com → drag and drop the image # Yandex
(often finds more matches than Google) https://yandex.com/images/search?rpt=imageview #
TinEye (exact match finder) https://tineye.com # CLI tool: gallery-dl + wget for batch
download of profile photos pip3 install gallery-dl gallery-dl
https://www.instagram.com/franciscomunoz/
```

3.2 EXIF Metadata Extraction | Location & Device Fingerprint

Photos posted online sometimes retain EXIF metadata containing GPS coordinates, device model, and timestamp. This data can confirm location and reveal the target's device — useful for cross-referencing with other profiles.

```
# Install exiftool sudo apt install libimage-exiftool-perl -y # Extract all metadata
from a downloaded image exiftool profile.jpg # Extract only GPS data exiftool -GPS*
profile.jpg # Batch process all images in a folder exiftool -r -GPS*
./downloaded_photos/ # Convert GPS coordinates to Google Maps URL # If GPS: 33 deg 26'
16.20" S, 70 deg 39' 1.20" W # → https://maps.google.com/?q=-33.4378,-70.6503
```

3.3 TikTok Search | Degree 0 — Younger Demographics

TikTok has become a primary platform for Chileans under 30. Its search API is accessible without login and often surfaces profiles that don't appear in Google results.

```
# Direct TikTok username search https://www.tiktok.com/@franciscomunoz # TikTok
internal search https://www.tiktok.com/search/user?q=Francisco+Munoz # CLI: check
TikTok with sherlock sherlock franciscomunoz --site tiktok --print-found # Socialscan —
checks username availability (if unavailable = account exists) pip3 install socialscan
socialscan franciscomunoz --platforms tiktok instagram twitter
```

3.4 LinkedIn OSINT | Professional Graph (Degree 1 — Coworkers)

LinkedIn exposes the professional graph — coworkers, employers, education institutions. For a Chilean university or workplace investigation, LinkedIn can reveal Degree 1 connections that are invisible on personal social networks.

```
# Google dork for LinkedIn (avoids login wall) site:linkedin.com/in "Francisco Munoz"
Chile site:linkedin.com/in "Francisco Munoz" Santiago # Find coworkers (Degree 1 — same
company) site:linkedin.com/in "Universidad" "Francisco Munoz" # Tool: linkedin2username
```

```
— generates username list from company employees pip3 install linkedin2username
linkedin2username -u your@email.com -c "company-slug" # CrossLinked — name-based
LinkedIn enumeration pip3 install crosslinked crosslinked -f
"{first}.{last}@company.com" "Company Name"
```

3.5 Wayback Machine | Deleted Profile Recovery

Profiles that have been deleted or made private may still be accessible through the Internet Archive's Wayback Machine. This is especially useful when Sherlock finds a URL that currently returns 404.

```
# Check if a deleted Instagram profile was ever archived curl
'http://archive.org/wayback/available?url=instagram.com/franciscomunoz' # Direct
Wayback URL https://web.archive.org/web/*/instagram.com/franciscomunoz # CLI: waybackpy
pip3 install waybackpy waybackpy --url 'https://instagram.com/franciscomunoz' --near
--year 2022
```

3.6 Socialscan | Username Availability = Account Exists

Socialscan checks username and email registration across platforms. If a username is 'unavailable' on a platform, an account exists — even if Sherlock couldn't confirm it due to rate limiting or bot detection.

```
pip3 install socialscan # Check username across key platforms socialscan franciscomunoz
fjmunoz fmunoz \ --platforms instagram twitter tiktok github reddit # Check email
registration socialscan francisco.munoz@gmail.com --platforms instagram twitter
```

3.7 theHarvester | Email & Subdomain Enumeration

theHarvester searches public data sources (Google, Bing, LinkedIn, Twitter, PGP keyservers) for emails and names associated with a domain. Useful when the target is associated with a company, university, or organization.

```
sudo apt install theharvester -y # Search for emails at a Chilean university domain
theHarvester -d udd.cl -b google,bing,linkedin -l 100 # Search specifically for a person
across all sources theHarvester -d gmail.com -b google -l 50 | grep -i 'francisco' #
Save to HTML report theHarvester -d udd.cl -b all -f results_harvester
```

3.8 Maltego CE | Visual Six Degrees Graph (Best for Presentation)

Maltego Community Edition is the gold standard for visual link analysis in academic OSINT. It automatically maps relationships between entities (people, emails, usernames, phone numbers) as a graph — making the Six Degrees model visually explicit and presentable.

```
# Install (requires free account at maltego.com) # Download from:
https://www.maltego.com/downloads/ sudo dpkg -i Maltego.v4.x.x.deb # Key transforms for
this experiment: # Person → 'To Social Networks' → finds Degree 0 profiles # Profile →
'To Affiliates' → finds Degree 1 connections # Email → 'To Person' → links email to
identity # Phone → 'To WhatsApp' → confirms WhatsApp presence # Best practice for
experiment: # 1. Create Person entity: 'Francisco Munoz' # 2. Run 'To Aliases' transform
# 3. Run 'To Social Networks' on each alias # 4. Screenshot the graph at each degree
level
```

4. Bayesian Confidence Scoring

Every profile found during the experiment must be scored using the Bayesian model. This transforms the qualitative investigation into a quantitative proof of the Six Degrees theory.

4.1 Scoring Formula

```
S = sum of (weight_i x match_i) Where match_i = 1 if evidence signal is present, 0 if absent Maximum possible score = 1.00 (all signals confirmed)
```

Evidence Signal	Weight	How to verify
Full name exact match	0.40	Profile name matches target name exactly
City / location match	0.25	Bio, posts, or check-ins show Santiago/Chile
Profile photo same person	0.20	Reverse image search confirms same photo elsewhere
Mutual friends / followers	0.10	Shared connections with already-confirmed profiles
Approximate age match	0.05	Birth year visible in bio, old posts, or school year

4.2 Confidence Thresholds

Score S	Level	Decision
S >= 0.85	Very High	Profile confirmed — include in graph as verified node
0.70 <= S < 0.85	High	Very likely — manually verify before including
0.50 <= S < 0.70	Medium	Possible match — collect more evidence signals
S < 0.50	Low	Unlikely — discard or flag as weak lead

4.3 Degree Weight Modifier

When scoring connections found in the graph (Degree 1, 2, 3), apply a proximity modifier to reflect the decreasing reliability of indirect associations:

```
Adjusted_Score = S x Degree_Weight Degree 0 (target): weight = 1.00 Degree 1 (direct friends): weight = 0.90 Degree 2 (friends of friends): weight = 0.65 Degree 3: weight = 0.40 Degree 4+: weight = 0.15
```

5. Experiment Execution Checklist

#	Action	Tool	Output
1	Install all tools (--install flag)	osint_experiment.sh	Tools ready
2	Generate username seed list	Username Anarchy	usernames.txt

3	Run fast platform sweep (top 5 usernames)	Sherlock	results_sherlock.txt
4	Run deep identity clustering	Maigret	PDF + HTML report
5	Test probable email addresses	Holehe	Platform list
6	Run Google dorks for real name	Browser	Profile URLs
7	Search Facebook People by name	Browser	Profile + friends
8	Verify phone on WhatsApp (if known)	curl + browser	Active/inactive
9	Run SpiderFoot for graph expansion	SpiderFoot web UI	Visual graph
10	Reverse image search profile photos found	Google/Yandex/TinEye	Cross-platform matches
11	Extract EXIF from downloaded photos	exiftool	GPS + device data
12	Check TikTok and LinkedIn	Sherlock + browser	Additional profiles
13	Check Wayback Machine for deleted profiles	waybackpy	Archived snapshots
14	Score each found profile (Bayesian)	osint_experiment.sh	confidence_scores.txt
15	Map graph: draw nodes and edges by degree	Manual / Maltego	Visual Six Degrees proof

6. Quick Command Reference Card

Tool	One-liner command
Username Anarchy	ruby ~/osint-tools/username-anarchy/username-anarchy.rb Francisco Munoz > usernames.txt
Sherlock	sherlock franciscomunoz fjmunoz --print-found --timeout 10 --output sherlock.txt
Maigret	maigret franciscomunoz --folderoutput ./maigret --report pdf --tags social
Holehe	holehe francisco.munoz@gmail.com --only-used
Google Dork	site:facebook.com "Francisco Munoz" Chile (in browser)
Facebook	https://www.facebook.com/search/people/?q=Francisco%20Munoz (in browser)
WhatsApp	curl -s -o /dev/null -w '%{http_code}' https://wa.me/56912345678
SpiderFoot	python3 -m spiderfoot -l 127.0.0.1:5001 (then open browser)
Socialscan	socialscan franciscomunoz fjmunoz --platforms instagram twitter tiktok
theHarvester	theHarvester -d udd.cl -b google,linkedin -l 100
exiftool	exiftool -GPS* profile.jpg
Waybackpy	waybackpy --url 'https://instagram.com/franciscomunoz' --near --year 2023
Maltego	GUI: Person entity → 'To Social Networks' → 'To Affiliates' transforms

7. Ethical & Legal Considerations

All techniques described in this document are based exclusively on publicly available information (OSINT). No technique requires bypassing authentication, accessing private data, or violating platform terms of service in ways that would constitute unauthorized access. In Chile, the Ley 19.628 (Protección de Datos Personales) and its 2024 update regulate the processing of personal data. This methodology is intended for legitimate investigative, academic, or security research purposes only. The investigator bears full responsibility for ensuring their use complies with applicable law.