

Open Source Intelligence

Presented by Shivam



CTF | Cyber Threat Intelligence Platform

Cannibals Strive to Stay Ahead of the Pack

ATT&CK® Navigator

MITRE ATT&CK®

attack.mitre.org

MITRE | ATT&CK®

Matrices | Tactics | Techniques | Defenses | CTI | Resources | Benefactors | Blog

Search

Reminder: the TAXII 2.0 server will be retiring on December 18. Please switch to the TAXII 2.1 server to ensure uninterrupted service.

ATT&CK®

Get Started

Contribute

FAQ

Take a Tour

Blog

Random Page

MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world — by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.

ATT&CK Matrix for Enterprise

layout: side | show sub-techniques | hide sub-techniques

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Communication
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	44 techniques	17 techniques	32 techniques	9 techniques	17 techniques	17 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (7)	Abuse Elevation Control Mechanism (6)	Abuse Elevation Control Mechanism (6)	Adversary-in-the-Middle (4)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (4)	Application Layer Protocol
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (11)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Cloud Infrastructure
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration	Boot or Logon Autostart Execution (14)	Account Manipulation (7)	BITS Jobs	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Malware
Gather Victim Network	Compromise Infrastructure (6)			Boot or Logon		Build Image on Host		Cloud Infrastructure Discovery		Automated	Communication

WHO AM I

Student

Former Gurugram cyber police Intern

Technical Content Manager at BSides Pune

Ethical Hacker & Malware Analyst

Intern at Cyber Secure India

Threat Hunter && Open Source Intelligence

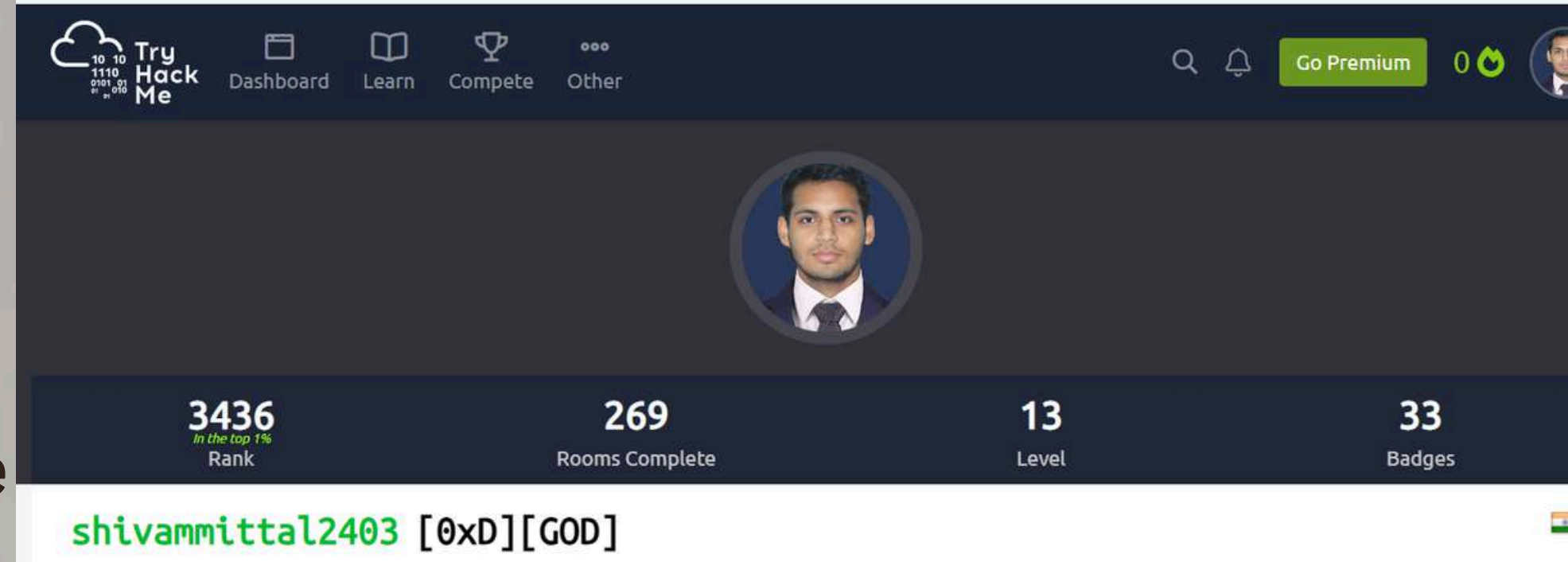
Analyst

Public Speaker

Car Hacking

Projects Like

- Airlines Hacking
- Ransomware Analysis
- PowerGrid Hacking
- Mobile Forensic
- Medical Hacking
- Data Privacy



Tools:

1. OSINT Tools
2. OSINT Tools 2
3. OSINT Tools 3
4. Threat Hunting OSINT tools

OMG 😱



**Be careful what you
share on social media!**

Final

PANO - Platform for Analysis and Network Operations | v8.1.5

NewSaveLoadWindows

Search for a helper

CircularHierarchicalRadialForce-Directed

Tools

Entities

Timeline

Company

Email

Image

Person

Phone

Text

Username

Vehicle

Website

Event

Location

Evidence

Entity 1

Entity 2

Entity 3

Entity 4

Entity 5

Entity 6

Entity 7

Entity 8

Entity 9

Entity 10

Entity 11

Entity 12

Entity 13

Entity 14

Entity 15

Entity 16

Entity 17

Entity 18

Entity 19

Entity 20

Entity 21

Entity 22

Entity 23

Entity 24

Entity 25

Entity 26

Entity 27

Entity 28

Entity 29

Entity 30

Entity 31

Entity 32

Entity 33

Entity 34

Entity 35

Entity 36

Entity 37

Entity 38

Entity 39

Entity 40

Entity 41

Entity 42

Entity 43

Entity 44

Entity 45

Entity 46

Entity 47

Entity 48

Entity 49

Entity 50

Entity 51

Entity 52

Entity 53

Entity 54

Entity 55

Entity 56

Entity 57

Entity 58

Entity 59

Entity 60

Entity 61

Entity 62

Entity 63

Entity 64

Entity 65

Entity 66

Entity 67

Entity 68

Entity 69

Entity 70

Entity 71

Entity 72

Entity 73

Entity 74

Entity 75

Entity 76

Entity 77

Entity 78

Entity 79

Entity 80

Entity 81

Entity 82

Entity 83

Entity 84

Entity 85

Entity 86

Entity 87

Entity 88

Entity 89

Entity 90

Entity 91

Entity 92

Entity 93

Entity 94

Entity 95

Entity 96

Entity 97

Entity 98

Entity 99

Entity 100

Entity 101

Entity 102

Entity 103

Entity 104

Entity 105

Entity 106

Entity 107

Entity 108

Entity 109

Entity 110

Entity 111

Entity 112

Entity 113

Entity 114

Entity 115

Entity 116

Entity 117

Entity 118

Entity 119

Entity 120

Entity 121

Entity 122

Entity 123

Entity 124

Entity 125

Entity 126

Entity 127

Entity 128

Entity 129

Entity 130

Entity 131

Entity 132

Entity 133

Entity 134

Entity 135

Entity 136

Entity 137

Entity 138

Entity 139

Entity 140

Entity 141

Entity 142

Entity 143

Entity 144

Entity 145

Entity 146

Entity 147

Entity 148

Entity 149

Entity 150

Entity 151

Entity 152

Entity 153

Entity 154

Entity 155

Entity 156

Entity 157

Entity 158

Entity 159

Entity 160

Entity 161

Entity 162

Entity 163

Entity 164

Entity 165

Entity 166

Entity 167

Entity 168

Entity 169

Entity 170

Entity 171

Entity 172

Entity 173

Entity 174

Entity 175

Entity 176

Entity 177

Entity 178

Entity 179

Entity 180

Entity 181

Entity 182

Entity 183

Entity 184

Entity 185

Entity 186

Entity 187

Entity 188

Entity 189

Entity 190

Entity 191

Entity 192

Entity 193

Entity 194

Entity 195

Entity 196

Entity 197

Entity 198

Entity 199

Entity 200

VEHICLE

Tesla Model S, 2023

MODEL: Tesla Model S

COLOR: Black

YEAR: 2023

VIN: 5YJ3E1EA5F000000000

NOTES: Registered under Dr. Foster's name

SOURCE: Vehicle Registration

PERSON

Dr. Jane Foster

FULLNAME: Dr. Jane Foster

AGE: 45

HEIGHT: 1.75

NATIONALITY: American

RESIDENCE: 420 W. Broadway St., NYC

EDUCATION: PhD in Physics

SOURCE: Professional ID

LOCATION

668 Coleridge Avenue, Palo Alto, CA 94304

ADDRESS: 668 Coleridge Avenue

CITY: Palo Alto

STATE: California

COUNTRY: United States

POSTAL_CODE: 94304

LATITUDE: 37.4418750

LONGITUDE: -122.1615122

LOCATION_TYPE: Residential

NOTES: Residence of Dr. Jane Foster

SOURCE: Google Maps

COMPANY

jane_foster_ai

WEBSITE: jane_foster.ai

PLATFORM: Twitter

LINK: https://twitter.com/jane_foster_ai

NOTES: Official Twitter account of Dr. Foster

SOURCE: Social Media

PHONE

+1-555-345-6789

NUMBER: +1-555-345-6789

PHONE_TYPE: Business

COUNTRY_CODE: +1

NOTES: Direct line of Dr. Foster

SOURCE: Company Directory

EVIDENCE

Patent Document

NAME: Patent Document

DESCRIPTION: Patent regarding revolutionary AI chip

NOTES: Filed by TechNova Inc.

SOURCE: Patent Office

TEXT

TechNova Inc. announced a rev...

TITLE: TechNova Inc. announced a rev...

URL: https://www.technova.com/news

NOTES: Official press release

SOURCE: Official website

IMAGE

Office Building Photo

TITLE: Office Building Photo

URL: https://www.technova.com/images

DESCRIPTION: A photo of TechNova Inc. building

NOTES: Captured during an official visit

SOURCE: Press release

EMAIL

contact@technova.com

ADDRESS: contact@technova.com

DOMAIN: technova.com

NOTES: Official contact email of TechNova Inc.

SOURCE: Company website

WEBSITE

TechNova Official Website

URL: https://www.technova.com

DOMAIN: technova.com

TITLE: TechNova Official Website

DESCRIPTION: Innovation through science

IP_ADDRESS: 192.168.1.1

STATUS: Active

TECHNOLOGIES: React, Node.js

NOTES: Primary company website

SOURCE: Data source: Intelligence

EVENT

AI Chip Launch Event

URL_TO_UPLOAD: 1

NAME: AI Chip Launch Event

DESCRIPTION: TechNova's unveiling of an advanced AI chip

START_DATE: 2025-02-07 10:00

END_DATE: 2025-02-07 13:00

NOTES: Major milestone for the company

SOURCE: Event invitation

Name: Me

Description: we been there whole

Start Time: 2025-02-07 23:43

End Time: 2025-02-07 23:43

Event Color: Select Color

Add Event

Entity 1

Entity 2

Entity 3

Entity 4

Entity 5

Entity 6

Entity 7

Entity 8

Entity 9

Entity 10

Entity 11

Entity 12

Entity 13

Entity 14

Entity 15

Entity 16

Entity 17

Entity 18

Entity 19

Entity 20

Entity 21

Entity 22

Entity 23

Entity 24

Entity 25

Entity 26

Entity 27

Entity 28

Entity 29

Entity 30

Entity 31

Entity 32

Entity 33

Entity 34

Entity 35

Entity 36

Entity 37

Entity 38

Entity 39

Entity 40

Entity 41

Entity 42

Entity 43

Entity 44

Entity 45

Entity 46

Entity 47

Entity 48

Entity 49

Entity 50

Entity 51

Entity 52

Entity 53

Entity 54

Entity 55

Entity 56

Entity 57

Entity 58

Entity 59

Entity 60

Entity 61

Entity 62

Entity 63

Entity 64

Entity 65

Entity 66

Entity 67

Entity 68

Entity 69

Entity 70

Entity 71

Entity 72

Entity 73

Entity 74

Entity 75

Entity 76

Entity 77

Entity 78

Entity 79

Entity 80

Entity 81

Entity 82

Entity 83

Entity 84

Entity 85

Entity 86

Entity 87

Entity 88

Entity 89

Entity 90

Entity 91

Entity 92

Entity 93

Entity 94

Entity 95

Entity 96

Entity 97

Entity 98

Entity 99

Entity 100

01/02/25 10:00

01/02/25 13:00

3h

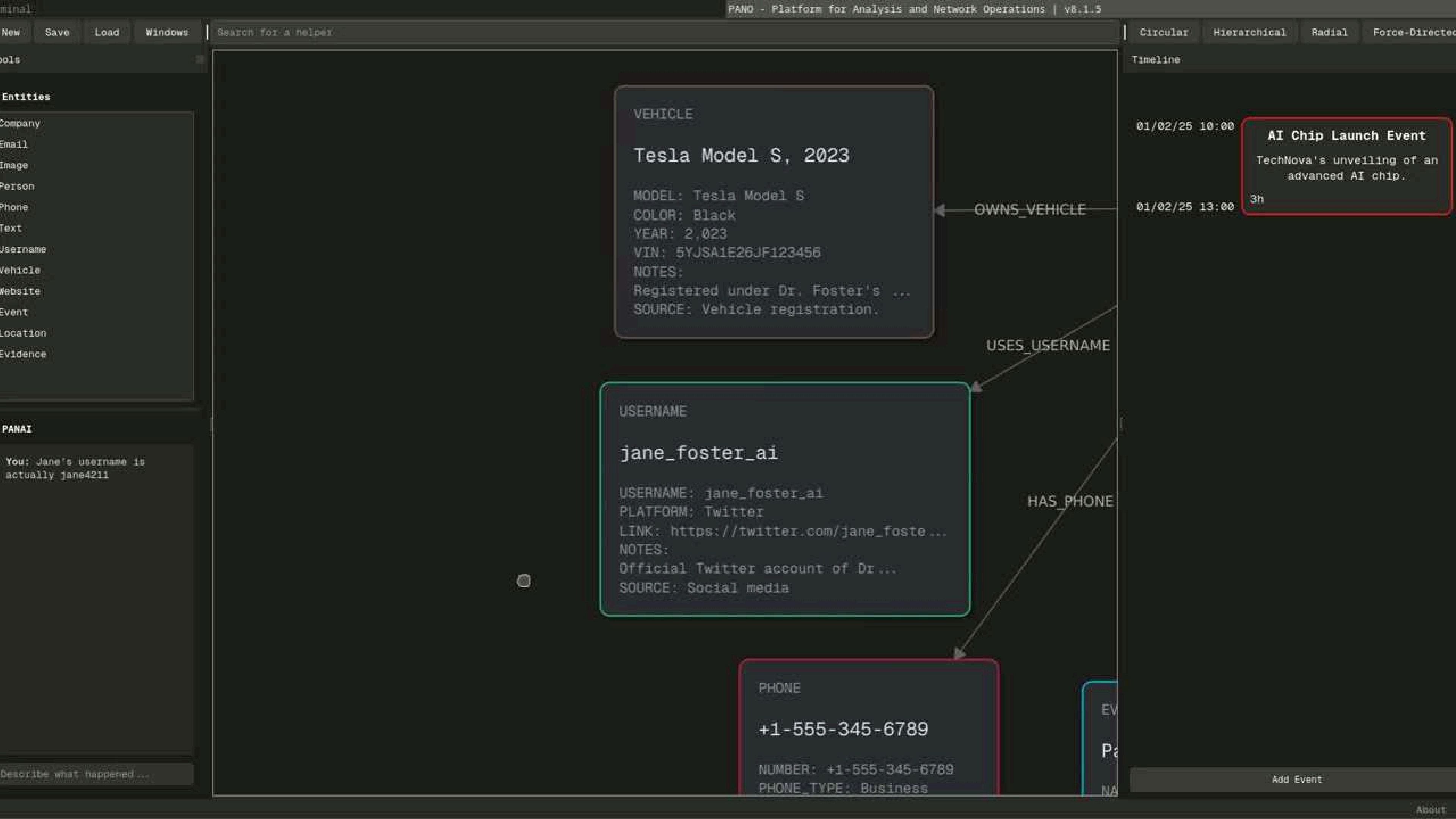
AI Chip Launch Event

TechNova's unveiling of an advanced AI chip.

Describe what happened...

Add Event

About



New Save Load Windows

Search for a helper

Circular

Hierarchical

Radial

Force-Directed

Tools

Timeline

Entities

Company

Email

Image

Person

Phone

Text

Username

Vehicle

Website

Event

Location

Evidence

PANA1

Media Analyzer

Deblurring

Perspective

File Controls

Upload Image

Save Result

Motion Blur Parameters

Angle (*): Draw 45

Length: 20

Thickness: 1.00



Original Image

Processed Image

Wiener Deconvolution Parameters

SNR: 40.00

Regularization: 0.0100

☐ Edge Padding☐ Auto SNR

Enhancement Parameters

Describe what happened...

Add Event

About

Evidence

Enter location of coordinates...

May 19, 2024

Describe what happened...

Force-Directed

Timeline

01/02/25 09:00

01/02/25 10:00

01/02/25 13:00

02/02/25 14:00

07/02/25 23:43

Don't know

AI Chip Launch Event

TechNova's unveiling of an advanced AI chip.

35

1d 5h

after 5d 9h 42mi

Me

I have been there whole
time

[Add Event](#)

New Save Load Windows

Search for a helper

Circular

Hierarchical

Radial

Force-Directed

Tools

Entities

Company

Email

Image

Person

Phone

Text

Username

Vehicle

Website

Event

Location

Evidence

PANAI

Describe what happened...

Text Translator

Source Text:

s

I

Detected Language: None

Target Language:

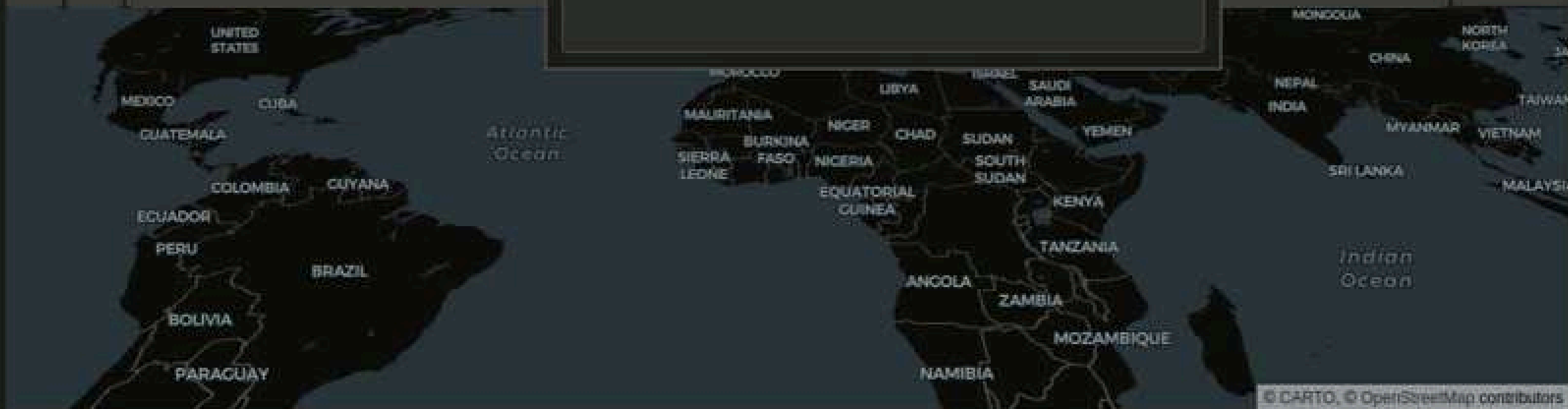
english

Translation:



Enter location or coordinates...

Search



Timeline

Add Event

About

Final

PANO - Platform for Analysis and Network Operations | v8.1.5

NewSaveLoadWindows

Search for a helper

CircularHierarchicalRadialForce-Directed

Tools

Entities

Timeline

Company

Email

Image

Person

Phone

Text

Username

Vehicle

Website

Event

Location

Evidence

VEHICLE

Tesla Model S, 2023

MODEL: Tesla Model S

COLOR: Black

YEAR: 2023

VIN: 5YJ3E1EA5FED540000

NOTES: Registered under Dr. Foster's name

SOURCE: Vehicle Registration

PERSON

Dr. Jane Foster

FULLNAME: Dr. Jane Foster

AGE: 45

HEIGHT: 1.75

NATIONALITY: American

RESIDENCE: 420 W. Broadway St., NYC

EDUCATION: PhD in Physics

SOURCE: Professional ID

LOCATION

668 Coleridge Avenue, Palo Alto, CA 94304

ADDRESS: 668 Coleridge Avenue

CITY: Palo Alto

STATE: California

COUNTRY: United States

POSTAL_CODE: 94304

LATITUDE: 37.4418750

LONGITUDE: -122.1615122

LOCATION_TYPE: Commercial

NOTES: Headquarters of TechNova Inc.

SOURCE: Google Maps

DOMAIN

jane_foster.ai

DOMAIN: jane_foster.ai

PLATFORM: Twitter

LINK: https://twitter.com/jane_foster_ai

NOTES: Official Twitter account of Dr. Foster

SOURCE: Social Media

PHONE

+1-555-345-6789

NUMBER: +1-555-345-6789

PHONE_TYPE: Business

COUNTRY_CODE: +1

NOTES: Direct line of Dr. Foster

SOURCE: Company Directory

EVIDENCE

Patent Document

NAME: Patent Document

DESCRIPTION: Patent regarding revolutionary AI chip

NOTES: Filed by TechNova's legal team

SOURCE: Patent Office

TEXT

TechNova Inc. announced a rev...

TITLE: TechNova Inc. announced a rev...

URL: https://www.technova.com/news

NOTES: Official press release

SOURCE: Official statement

EMAIL

contact@technova.com

ADDRESS: contact@technova.com

DOMAIN: technova.com

NOTES: Official contact email of TechNova

SOURCE: Company website

WEBSITE

TechNova Official Website

URL: https://www.technova.com

DOMAIN: technova.com

TITLE: TechNova Official Website

DESCRIPTION: Revolutionary technology solutions for tomorrow's world

STATUS: Active

REGISTRATION: 2018-01-15

NOTES: Primary company website

SOURCE: Web archive / Intelligence

EVENT

AI Chip Launch Event

NAME: AI Chip Launch Event

DESCRIPTION: TechNova's unveiling of an advanced AI chip

START_DATE: 2025-02-07 10:00

END_DATE: 2025-02-07 13:00

NOTES: Major milestone for the company

SOURCE: Event invitation

ADD EVENT

Name: Me

Description: ve been there whole

Start Time: 2025-02-07 23:43

End Time: 2025-02-07 23:43

Event Color: Select Color

Add Event

IMAGE

Office Building Photo

TITLE: Office Building Photo

URL: https://www.technova.com/building

DESCRIPTION: A photo of TechNova's new office building

NOTES: Captured during an official visit

SOURCE: Press release

Relationships

owns vehicle

uses software

has phone

submitted

located at

hosted event

has website

Timeline

01/02/25 10:00

01/02/25 13:00

AI Chip Launch Event

TechNova's unveiling of an advanced AI chip.

3h

You: create an example case with all the entities given

PANAI: Changes made:

PANAI: - Company: TechNova Inc.

PANAI: - Email: contact@technova.com

PANAI: - Image: Office Building Photo

PANAI: - Person: Dr. Jane Foster

PANAI: - Phone: +1-555-345-6789

PANAI: - Text: TechNova Inc. announced a revolutionary AI chip today.

PANAI: - Username: jane_foster.ai

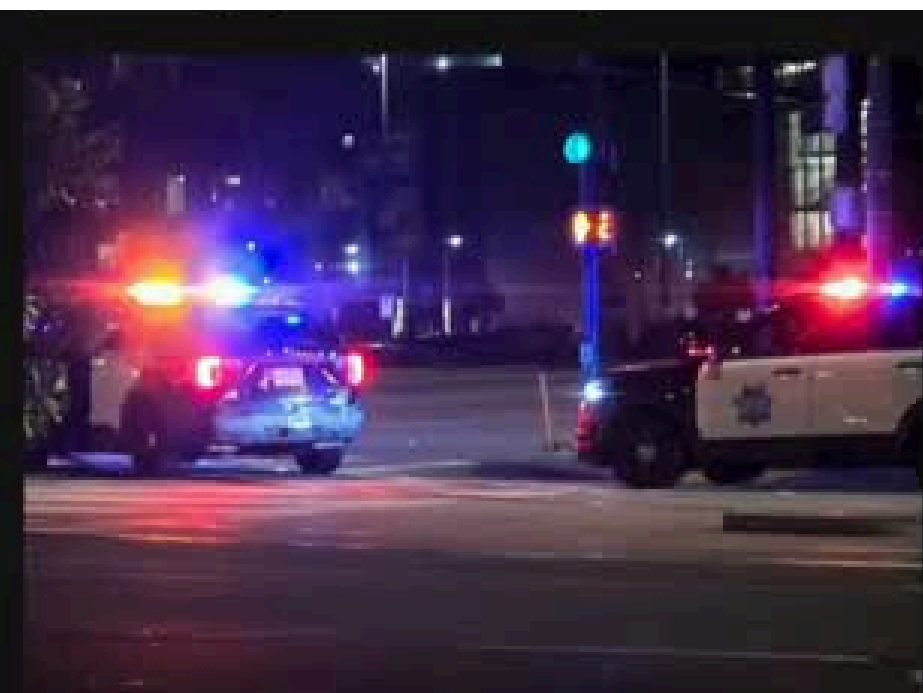
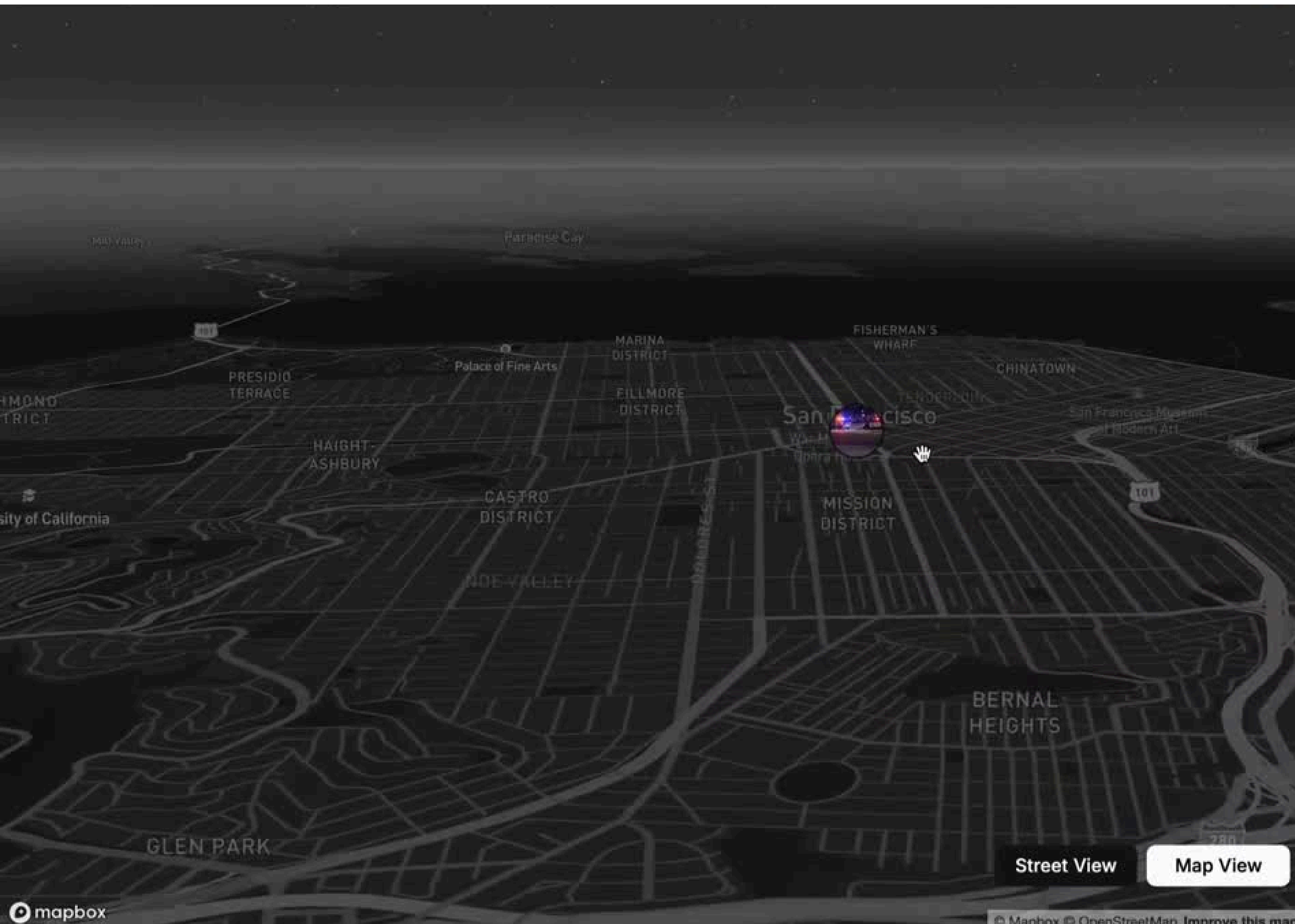
PANAI: - Vehicle: Tesla Model S, 2023

PANAI: - Website: TechNova

Describe what happened...

Add Event

About



The police cars have "SFPD" markings, which stands for San Francisco Police Depa...

Latitude:
37.7749

Longitude:
-122.4194



City:
San Francisco

Country:
United States

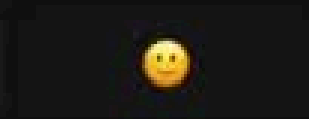
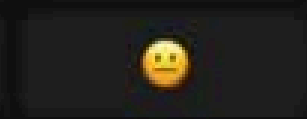
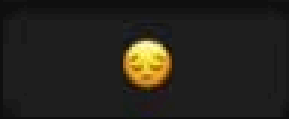
Camera Type:
samsung

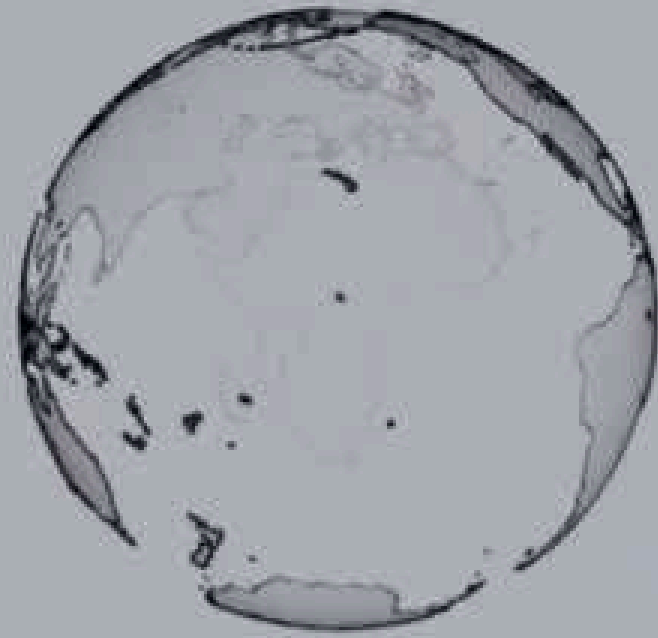
Camera Model:
Galaxy S24 Ultra

Export PDF

Share Geospy

How'd we do?



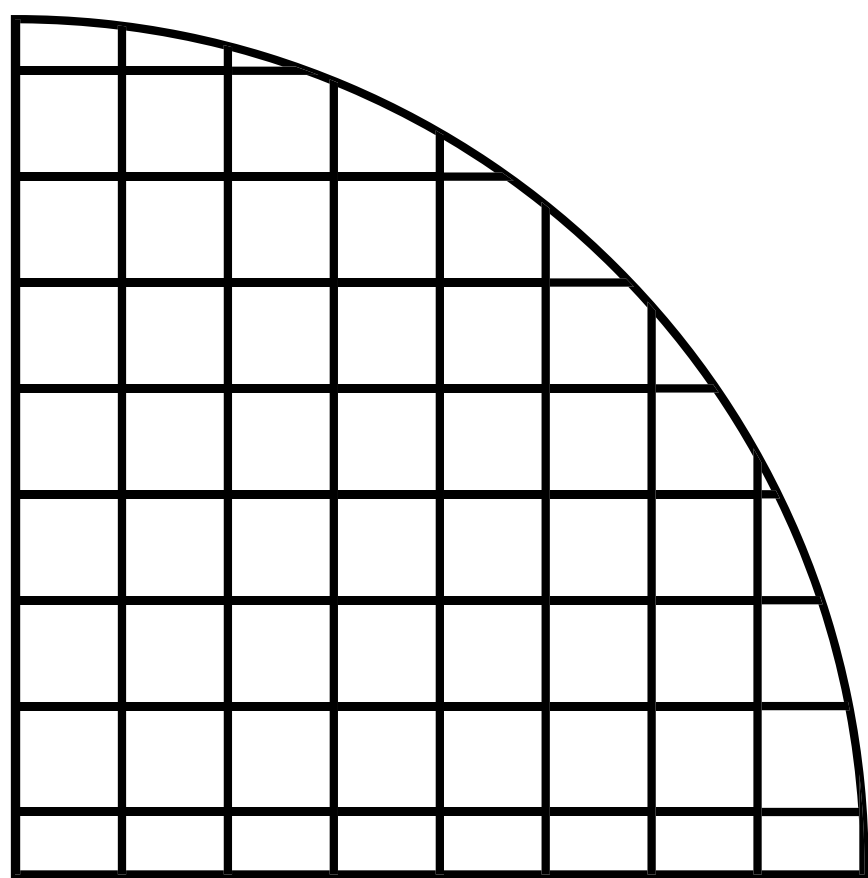


Covert Cabal

Case Study #1: Tracking the Suez Canal Blockage in 2021

Case Study #2: Belarus Arrested Dissident Journalist

Case Study #3: Master OTW's Unveiling Mastermind Behind Global Scam



What is OSINT

Open Source Intelligence (OSINT) refers to the collection, processing, and dissemination of publicly available information from various sources, including the internet, social media, news outlets, and other publicly accessible materials.



What is Data ?

Types of Data

- Structured
- Unstructured
- Semi structured

```
"created_at": "2024-03-03T12:57:44+05:30",
"updated_at": "2024-03-03T13:56:48+05:30",
"first_name": "Pravesh Ranawat",
"last_name": null,
"orders_count": 1,
"state": "enabled",
"total_spent": "1484.00",
"last_order_id": 5955407577186,
"note": null,
"verified_email": true,
"multipass_identifier": null,
"tax_exempt": false,
"tags": "Created an account, eligible for sign up bonus",
"last_order_name": "#6259593",
"currency": "INR",
"phone": "+919636402216",
"addresses": [
  {
    "id": 9004128174178,
    "customer_id": 7661421428834,
    "first_name": "Pravesh",
    "last_name": ".",
    "company": null,
    "address1": "B wing tcs kenington building 5th floor ODC C",
    "address2": null,
    "city": "MUMBAI",
    "province": "Maharashtra",
    "country": "India",
    "zip": "400076",
    "phone": "9636402216",
    "name": "Pravesh .",
    "province_code": "MH",
```

```
5:23 PM
},
"sms_marketing_consent": {
  "state": "not_subscribed",
  "opt_in_level": "single_opt_in",
  "consent_updated_at": null,
  "consent_collected_from": "OTHER"
},
"admin_graphql_api_id": "gid://shopify/Customr/7661420281954"
},
{
  "id": 7661420150882,
  "email": "niveditachoudhary2000@gmail.com",
  "created_at": "2024-03-03T12:56:34+05:30",
  "updated_at": "2024-03-03T13:04:45+05:30",
  "first_name": "Nivedita",
  "last_name": null,
  "orders_count": 0,
  "state": "enabled",
  "total_spent": "0.00",
  "last_order_id": null,
  "note": null,
  "verified_email": true,
  "multipass_identifier": null,
  "tax_exempt": false,
  "tags": "Created an account, eligible for sign up bonus",
  "last_order_name": null,
  "currency": "INR",
  "phone": "+919654776817",
  "addresses": [],
  "tax_exemptions": ~/do~/download~/dow
~/downloads $
```


Personal, Professional, and Financial Information

1. Personal Information

- Identity: Name, Birth Details, Gender, Nationality
- Contact: Address, Phone Numbers, Emails
- IDs: National ID, Passport, Driver's License

2. Family and Relationships

- Family Details: Parents, Siblings, Spouse, Children
- Emergency Contacts: Close Relatives or Friends

3. Education and Training

- Academic: School, College Degrees, Transcripts
- Certifications: Professional and Online Course Certificates

4. Employment and Career

- Resume/CV: Job History, Skills, Achievements
- Contracts: Employment Agreements, NDAs
- Reviews: Appraisals and Feedback

5. Financial Information

- Banking: Account Details, Credit Cards
- Income & Taxes: Salary Slips, Tax Returns
- Debts: Loans, Mortgage Details

6. Health and Medical

- Medical Records: Health History, Vaccination, Reports
- Insurance: Health and Life Insurance Policies
- Prescriptions: Ongoing Medications

Personal, Professional, and Financial Information

7. Legal Information

- Wills & Trusts: Testament, Living Trust Documents
- Contracts: Rental, Business Agreements
- Legal Docs: Power of Attorney, Marriage Certificates

8. Property and Assets

- Real Estate: Property Deeds, Mortgage Documents
- Personal Property: Vehicle Registration, Valuables
- Digital Assets: Online Account Credentials, Cryptocurrency

9. Social and Community

- Social Media: Account Details, Content
- Memberships: Clubs, Organizations
- Volunteer Work: Community Service Records

10. Technology and Digital Life

- Devices: Serial Numbers, Purchase Details
- Software: Licenses
- Online Presence: Website, Blogs

11. Psychological Profiling

- Personality Traits: Personality Tests (e.g., MBTI, Big Five)
- Behavioral Patterns: Habits, Routines, and Behavioral Analysis
- Emotional Profile: Stress Levels, Emotional Triggers, Coping Mechanisms
- Mental Health: History of Mental Health Conditions, Therapy, and Counseling Records
- Motivations and Goals: Personal and Professional Aspirations, Life Goals
- Risk Assessment: Psychological Risks, Potential for Harmful Behavior

When is Open Source Intelligence used?

Open Source Intelligence (OSINT) is utilized in various fields, each with a unique focus:

1. **National Security:** OSINT helps identify threats like terrorism or cyber-attacks, ensuring timely interventions.
2. **Business Intelligence:** Companies leverage OSINT to understand market trends, analyze competitors, and track consumer behavior.
3. **Law Enforcement:** It aids in criminal investigations, suspect tracking, and dismantling criminal networks.
4. **Military Operations:** Military forces use OSINT to gather intelligence on enemy strategies and troop movements.
5. **Humanitarian Response:** OSINT provides critical information during natural disasters, conflicts, or humanitarian crises.
6. **Business Development:** It's instrumental in identifying growth opportunities, monitoring competitors, and staying updated with market trends.

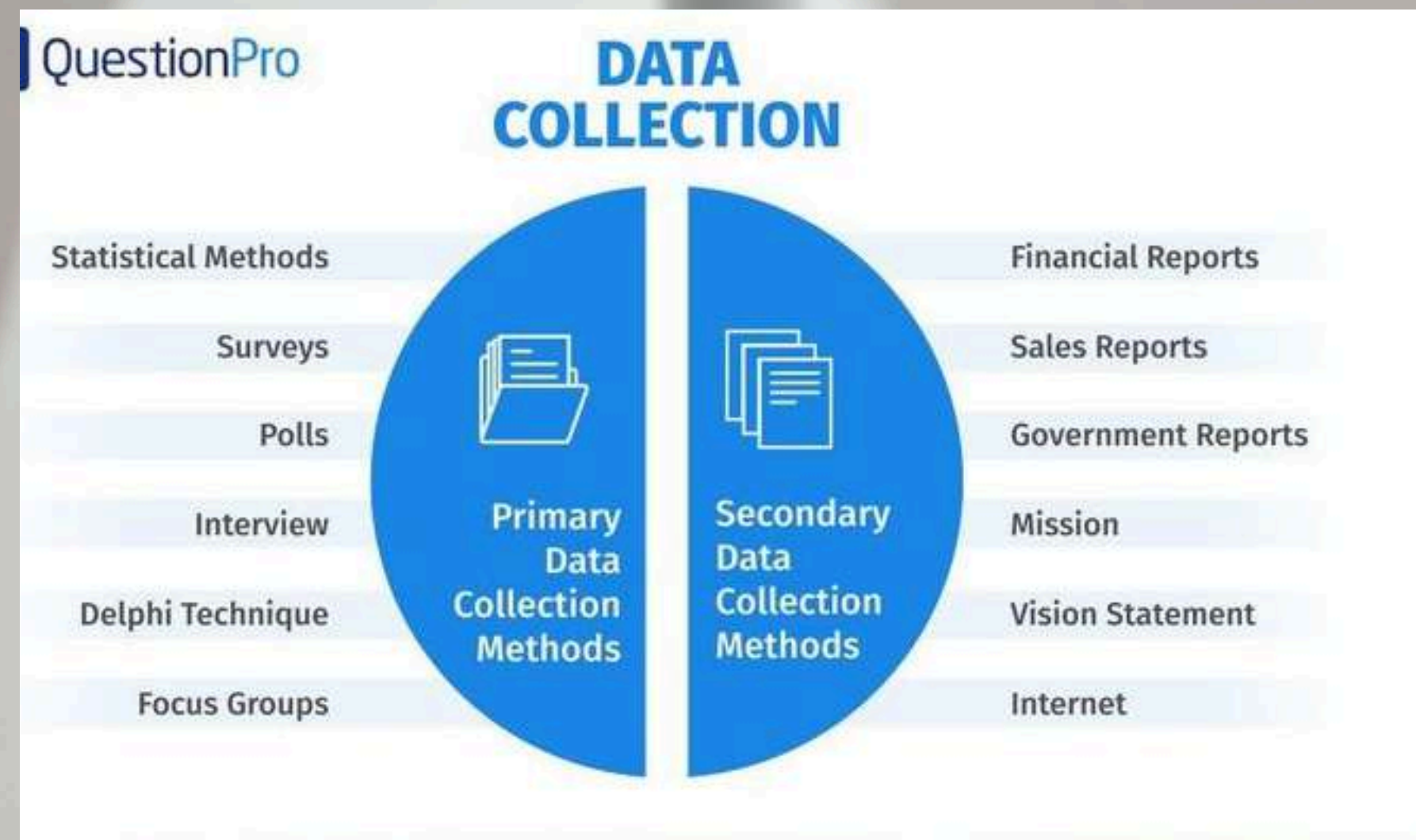
Israel Says It Killed Hezbollah Commander in Airstrike Near Beirut

The strike was in retaliation for a deadly rocket attack this weekend in the Golan Heights. At least three civilians were killed and 74 others wounded on Tuesday, Lebanese officials said.

How is Open Source Intelligence collected?

Open Source Intelligence (OSINT) can be gathered through various techniques, each providing unique insights:

1. **Web Scraping:** Extracting data from websites, forums, and social media platforms.
2. **Social Media Monitoring:** Tracking conversations, hashtags, and mentions across social networks.
3. **News Aggregation:** Collecting news articles and reports from reputable sources.
4. **Public Records Search:** Accessing court documents, property records, and company filings.
5. **Open-Source Data Collection:** Utilizing publicly available sources, such as government databases and open-source datasets.



Who uses Open Source Intelligence?

OSINT is a powerful tool utilized by a variety of entities, often with a strategic or investigative edge:

1. **Government Agencies:** Intelligence agencies, law enforcement, and military organizations tap into OSINT for national security, criminal investigations, and defense strategies.
2. **Businesses:** Companies across industries, including finance, technology, and healthcare, use OSINT for competitive analysis, market insights, and risk management.
3. **Non-Profit Organizations:** Advocacy groups, human rights organizations, and other non-profits employ OSINT to uncover injustices, monitor conflicts, and gather evidence.
4. **Individuals:** Journalists, researchers, and private investigators harness OSINT to dig deep, uncover hidden truths, and craft compelling narratives.



Why is Open Source Intelligence important?

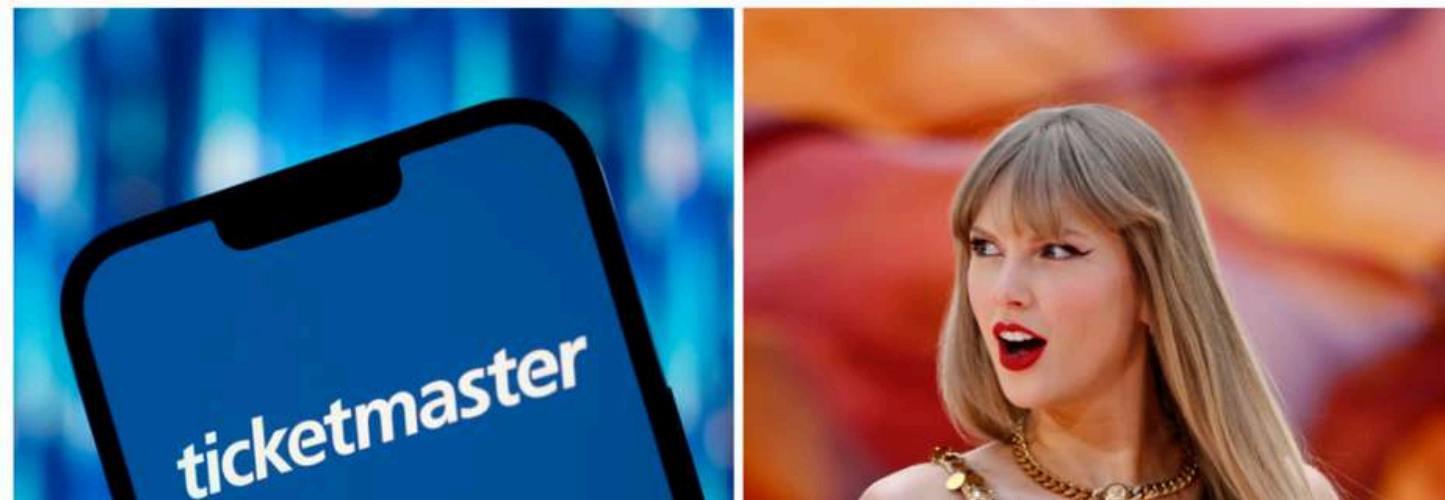
Why OSINT is Crucial?

1. **Unveils Hidden Truths:** OSINT pierces the veil, revealing insights into market dynamics or lurking security threats that others might miss.
2. **Exploits Efficiency:** Traditional intelligence methods are slow and costly. OSINT, however, slices through time and budget constraints, delivering information swiftly and economically.
3. **Heightens Vigilance:** In a world of constant change, OSINT sharpens an organization's awareness, ensuring they remain steps ahead, ready to act on informed decisions.

Ticketmaster hackers are holding data of 440,000 Taylor Swift ticketholders for ransom

The hackers have upped their ransom demand to \$8 million.

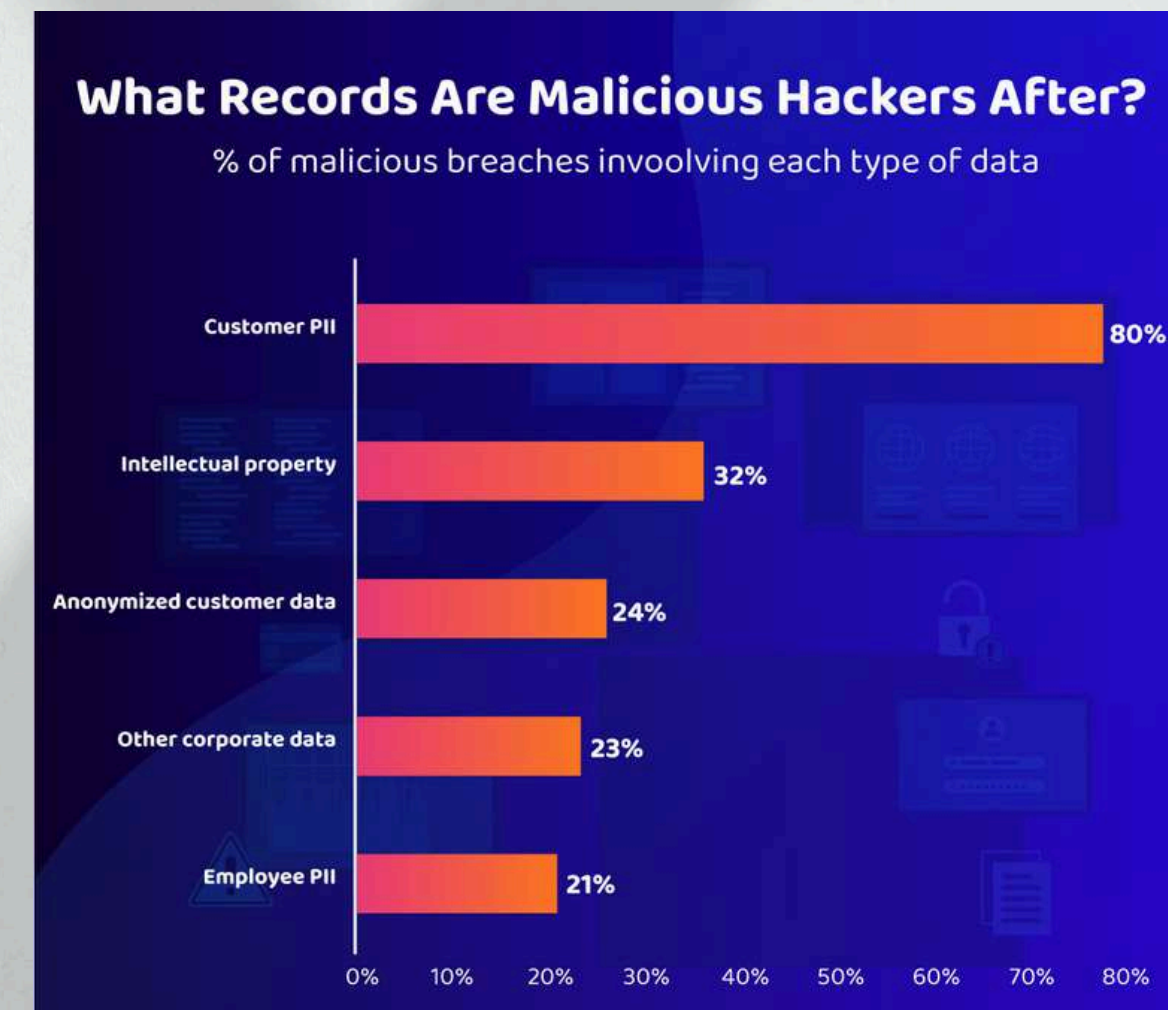
By [Amanda Yeo](#) on July 5, 2024



Where is Open Source Intelligence used?

OSINT - Across the Globe:

1. **North America: Powerhouses** like the **United States** and **Canada** heavily utilize OSINT for national security and corporate intelligence.
2. **Europe:** Countries such as the **UK, Germany,** and **France** leverage OSINT for everything from counterterrorism to business analysis.
3. **Asia-Pacific:** Nations like **Japan, China,** and **Australia** are increasingly integrating OSINT into their strategic frameworks.
4. **Latin America:** Countries like **Brazil** and **Mexico** are adopting OSINT to enhance security measures and economic insights.



Where is Open Source Intelligence used?

Examples of Open Source Intelligence:

1. **Tracking Terrorist Organizations:** Leveraging social media and online forums to monitor activities of groups like **ISIS** or **Al-Qaeda**.
2. **Monitoring Market Trends:** Analyzing social media, news, and industry reports to gauge market trends and consumer behavior.
3. **Investigating Crimes:** Utilizing public records and online archives to investigate crimes, trace suspects, or map criminal networks.

300 Indian banks hit after ransomware attack cripples payment systems: Report

A ransomware attack on a service provider of banking technology systems has temporarily shut down nearly 300 small banks across India. An audit was being conducted to ensure the attack does not spread further.

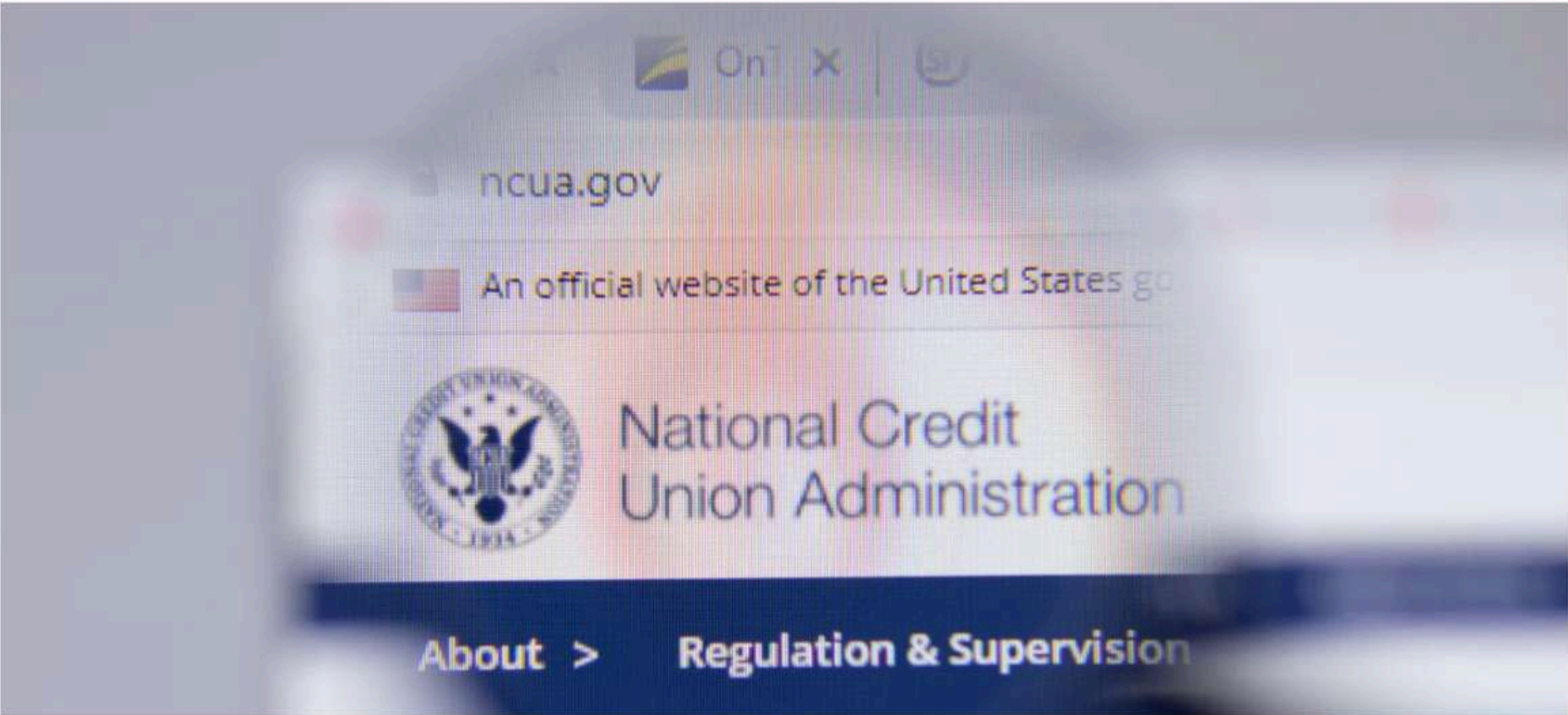
Listen to Story Share



Ransomware attack causes outages at 60 credit unions, federal agency says

By Sean Lyngaas, CNN
2 minute read · Updated 11:06 AM EST, Mon December 4, 2023

f X e



MORE FROM CNN



NEWS & BUZZ

OSINT Techniques

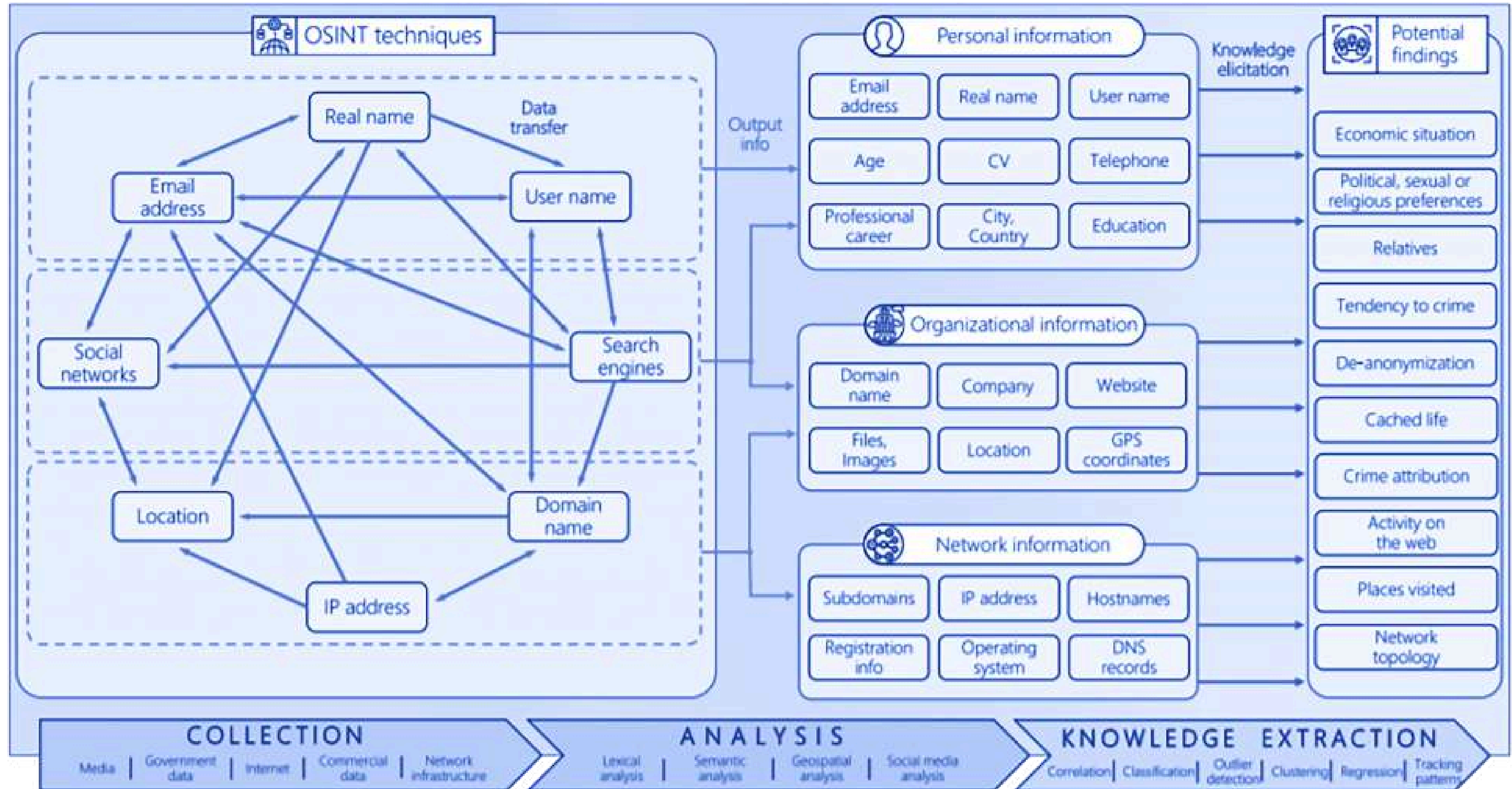
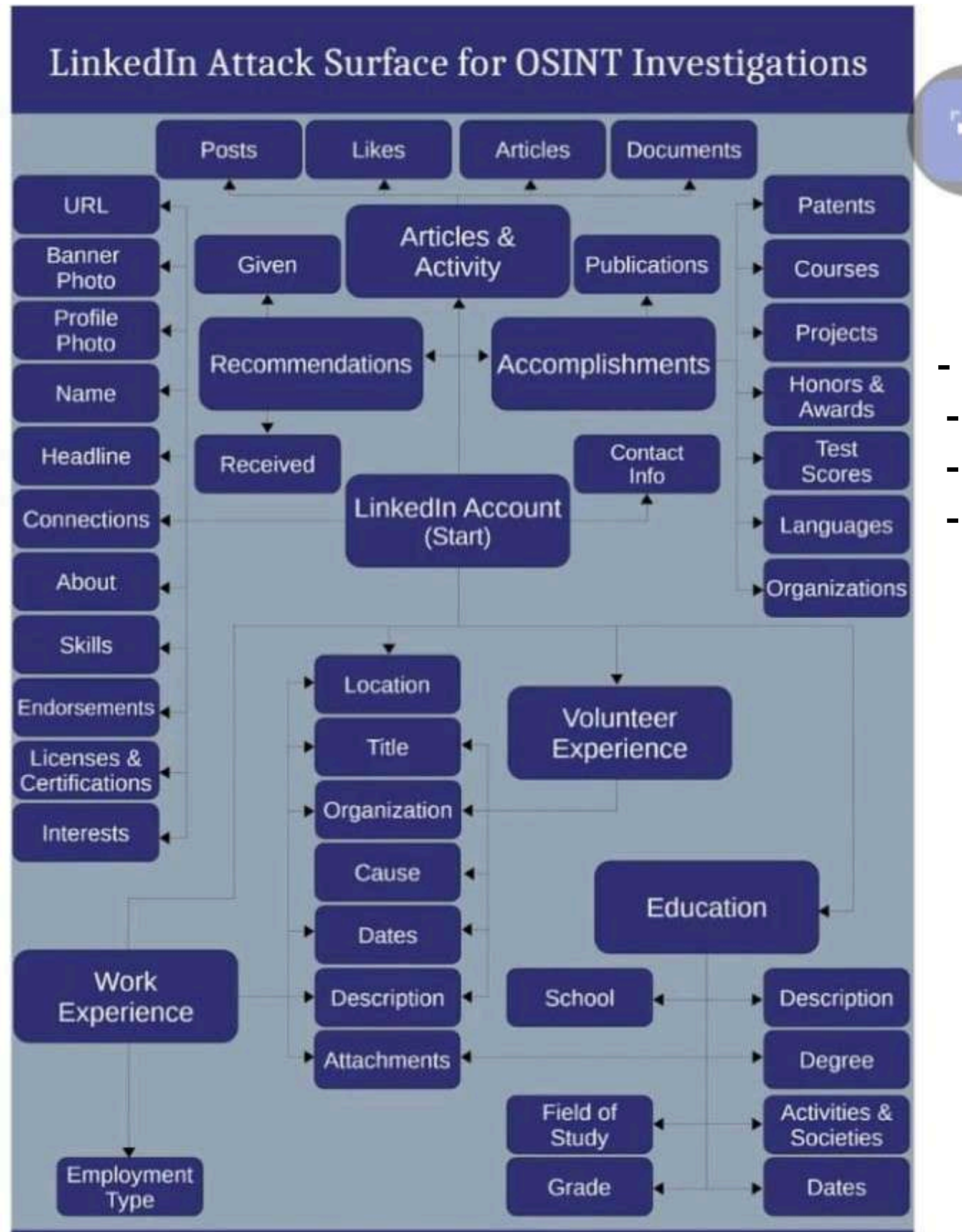


FIGURE 2. Principal OSINT workflows and derived intelligence.



LinkedIn OSINT

- Introduces LinkedIn OSINT for gathering professional intelligence.
- Discusses analyzing connections, endorsements, and employment history.
- Highlights risks of public LinkedIn data exposure.
- Suggests ways to secure LinkedIn profiles from intelligence gathering.

1. LinkedIn OSINT

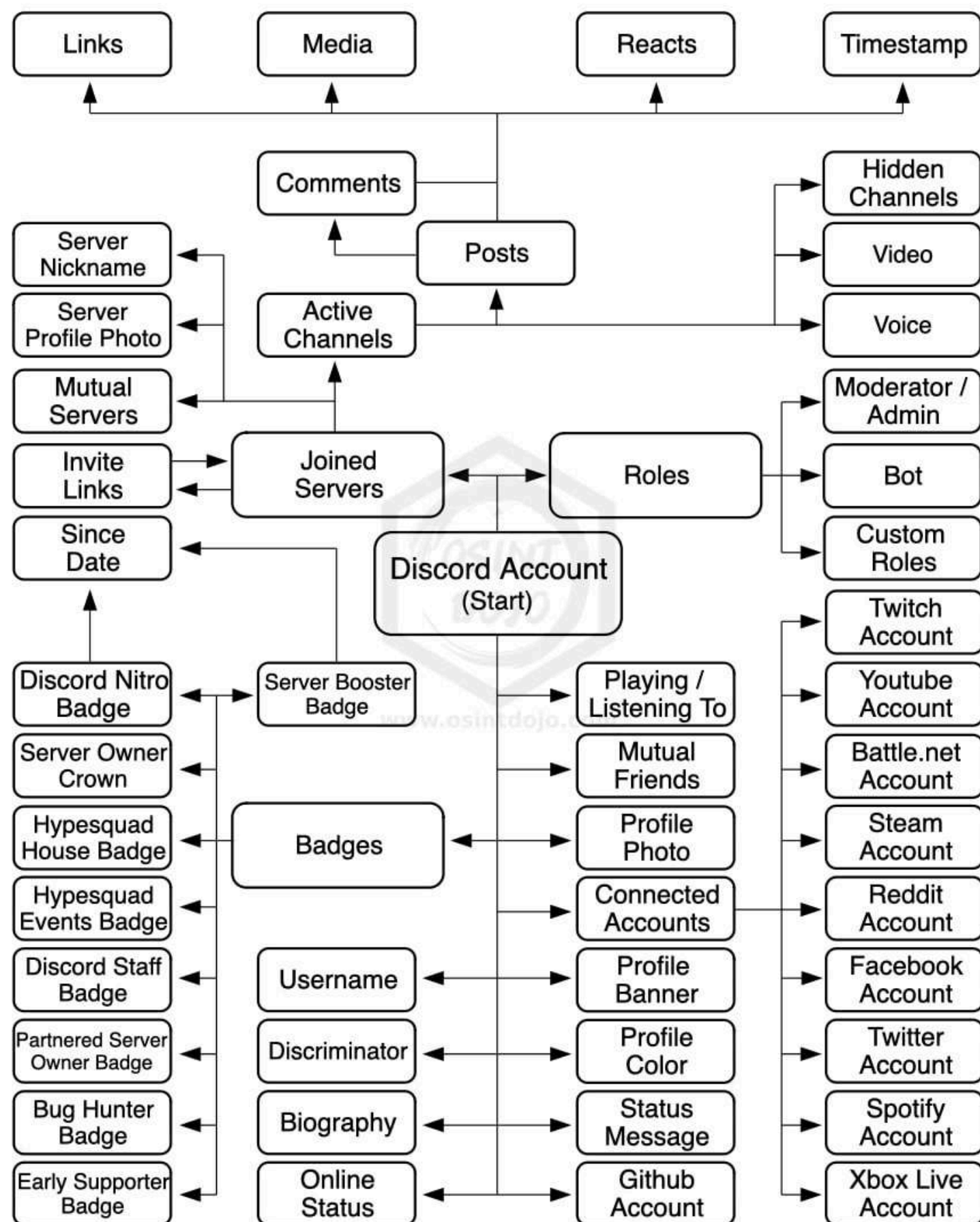
- Tools:
 - Maigret – Scrapes LinkedIn profiles.
 - theHarvester – Extracts emails, names, subdomains, and social media data.
 - LinkedInt – Advanced LinkedIn scraper.
 - Socinator – LinkedIn automation and intelligence tool.
- Exploits:
 - Open profiles expose employment history and corporate links.
 - Third-party plugins may leak data (e.g., browser extensions).
- News:
 - 2023: 500M LinkedIn profiles leaked on hacking forums.

Discord OSINT

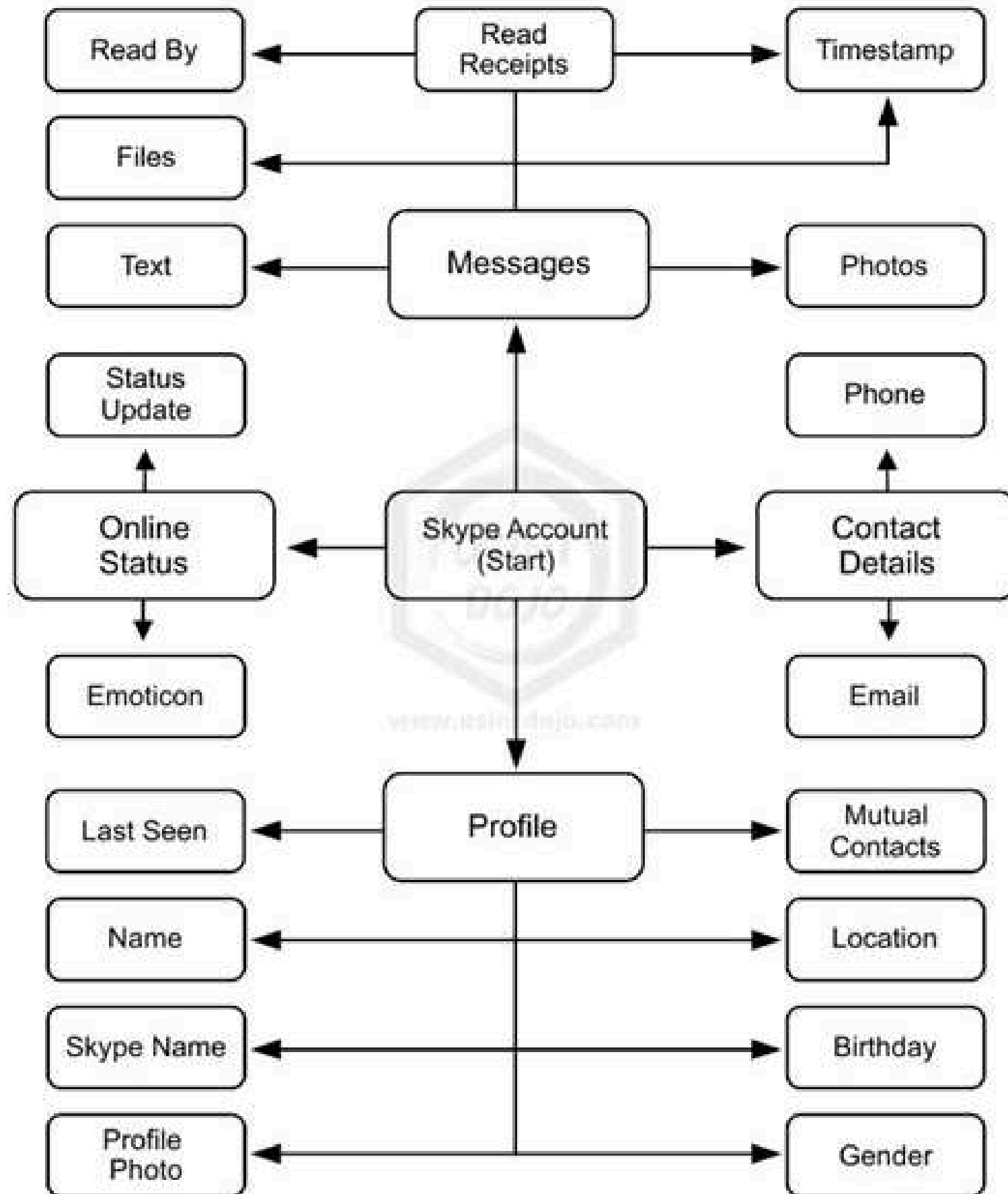
- Covers Discord OSINT, focusing on tracking user activity in servers.
- Discusses monitoring messages, roles, and permissions for intelligence.
- Identifies Discord as a platform for cybercriminal discussions.
- Suggests ethical guidelines for Discord-based intelligence gathering.

2. *Discord OSINT*

- **Tools:**
 - **Discord History Tracker** – Logs all messages from a server.
 - Sn0int – Extracts usernames and Discord data.
 - DiscoRipper – Scrapes servers and messages.
- **Exploits:**
 - Discord API leaks user activity timestamps.
 - Malicious bots collect user data.
- **News:**
 - 2024: Discord hacked, exposing internal developer accounts.



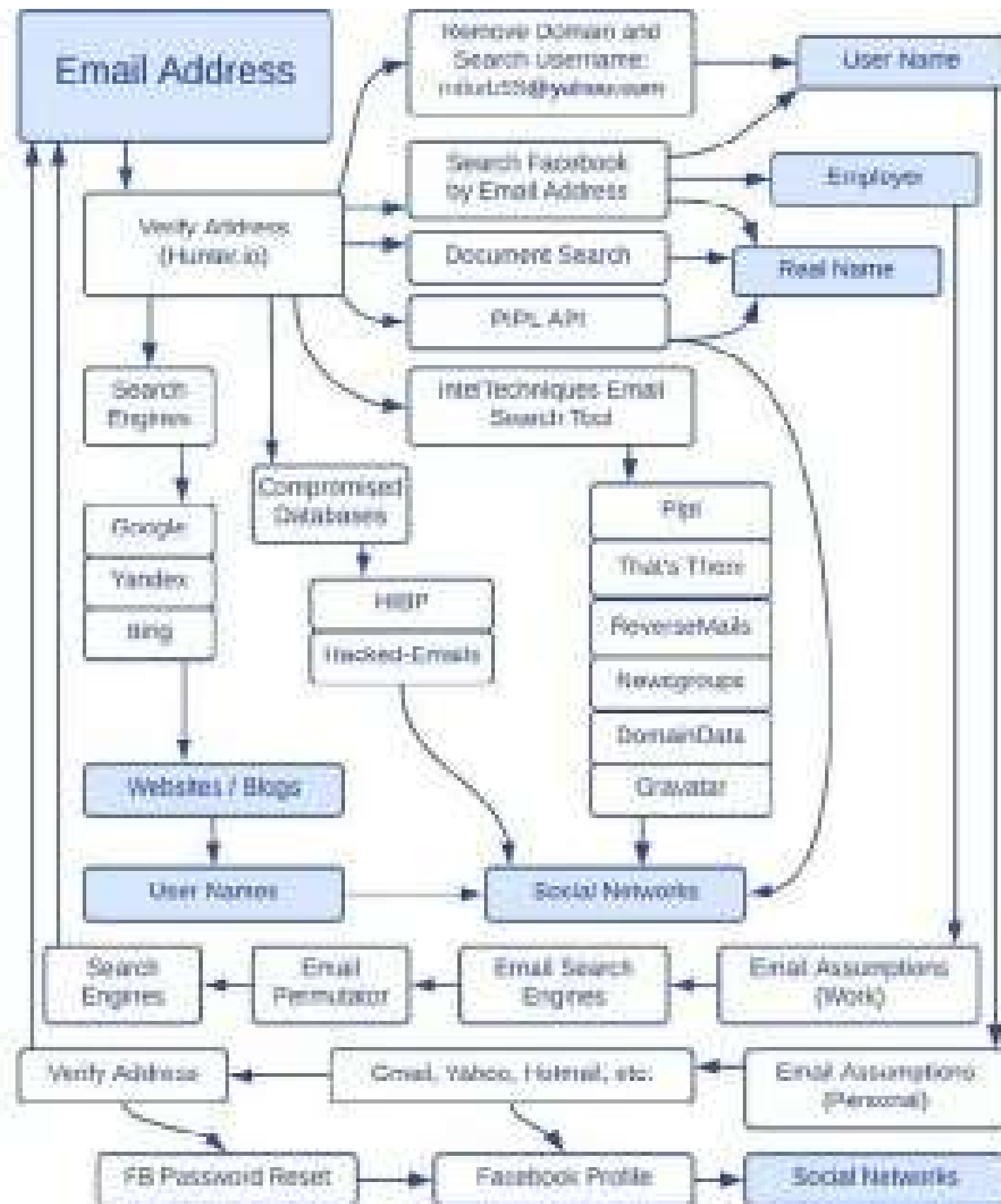
Skype OSINT



- Explains Skype OSINT and how metadata from calls and messages can be analyzed.
- Discusses retrieving usernames and activity timestamps.
- Highlights vulnerabilities in Skype's security that could expose user data.
- Recommends securing Skype accounts against OSINT tracking.

3. Skype OSINT

- Tools:
 - Skype Resolver – Finds IP from a Skype username.
 - OSINT Framework – Collects Skype-related metadata.
- Exploits:
 - Leaked credentials allow session hijacking.
 - Call metadata reveals caller locations.
- News:
 - 2023: Microsoft confirmed an exploit leaking Skype IP addresses.



Email Osint

- Introduces Email OSINT, including techniques for email header analysis.
- Covers tracing the sender's IP and detecting phishing attempts.
- Discusses tools used for email forensics.
- Suggests security practices to protect email accounts from OSINT threats.

📞 Communication & Personal Data OSINT

6. Email OSINT

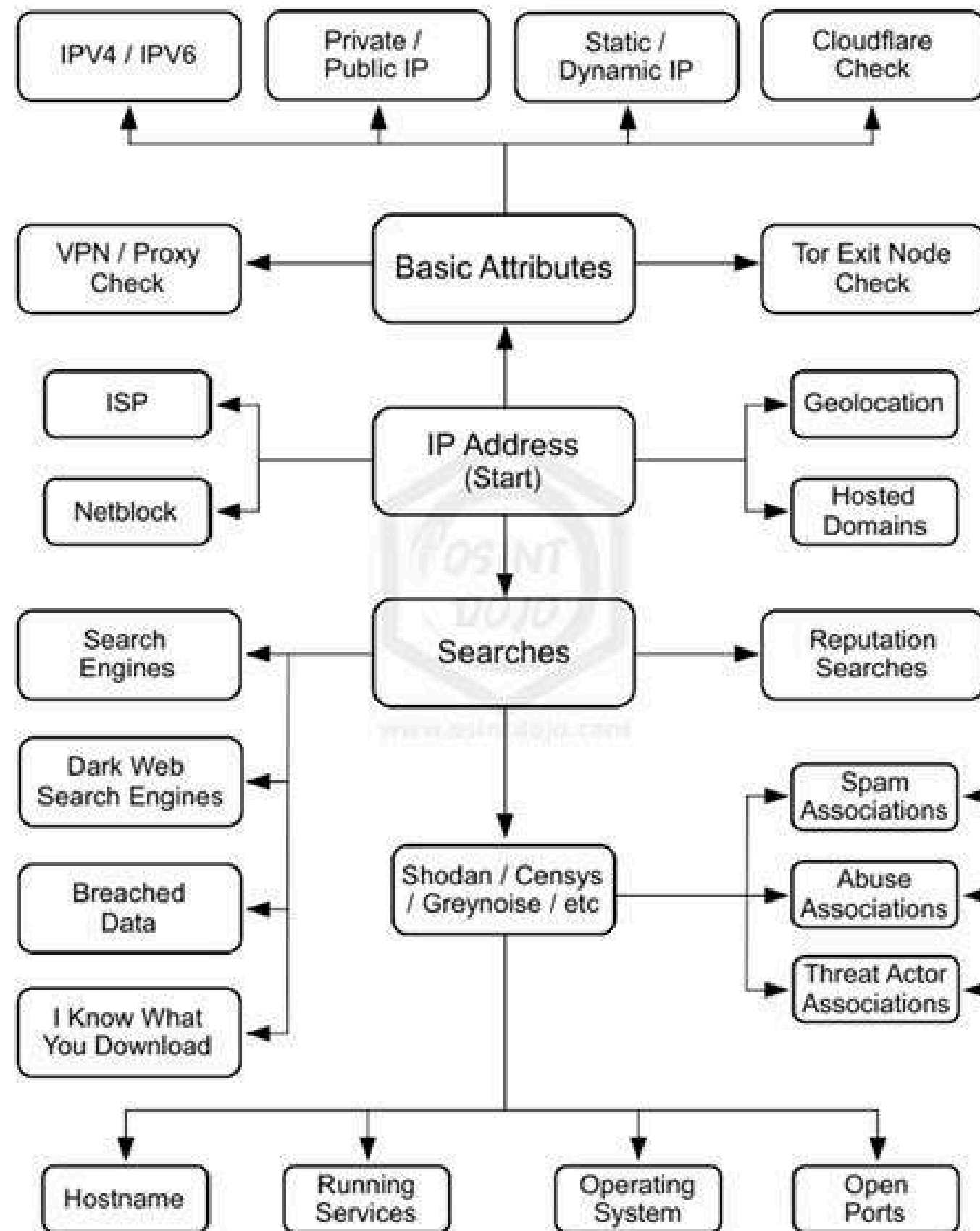
- Tools:
 - Have I Been Pwned – Checks if an email was leaked.
 - Holehe – Finds accounts linked to an email.
 - OSINT.email – Extracts metadata from email headers.
- Exploits:
 - SPF/DKIM misconfigurations allow spoofing.
- News:
 - 2023: Google updated its DMARC policies after a major spoofing attack.

IP Address

- Discusses IP Address OSINT and how geolocation tracking works.
- Covers methods for identifying the owner of an IP address.
- Explains how VPNs and proxies can mask IP addresses.
- Suggests best practices for hiding IP information from OSINT tools.

10. IP Address OSINT

- Tools:
 - IPinfo.io – Geolocation lookup.
 - Onyphe – Dark web intelligence on IPs.
- Exploits:
 - Exposed VPN servers allow tracking.
- News:
 - 2023: FBI seized multiple IP-based tracking services.

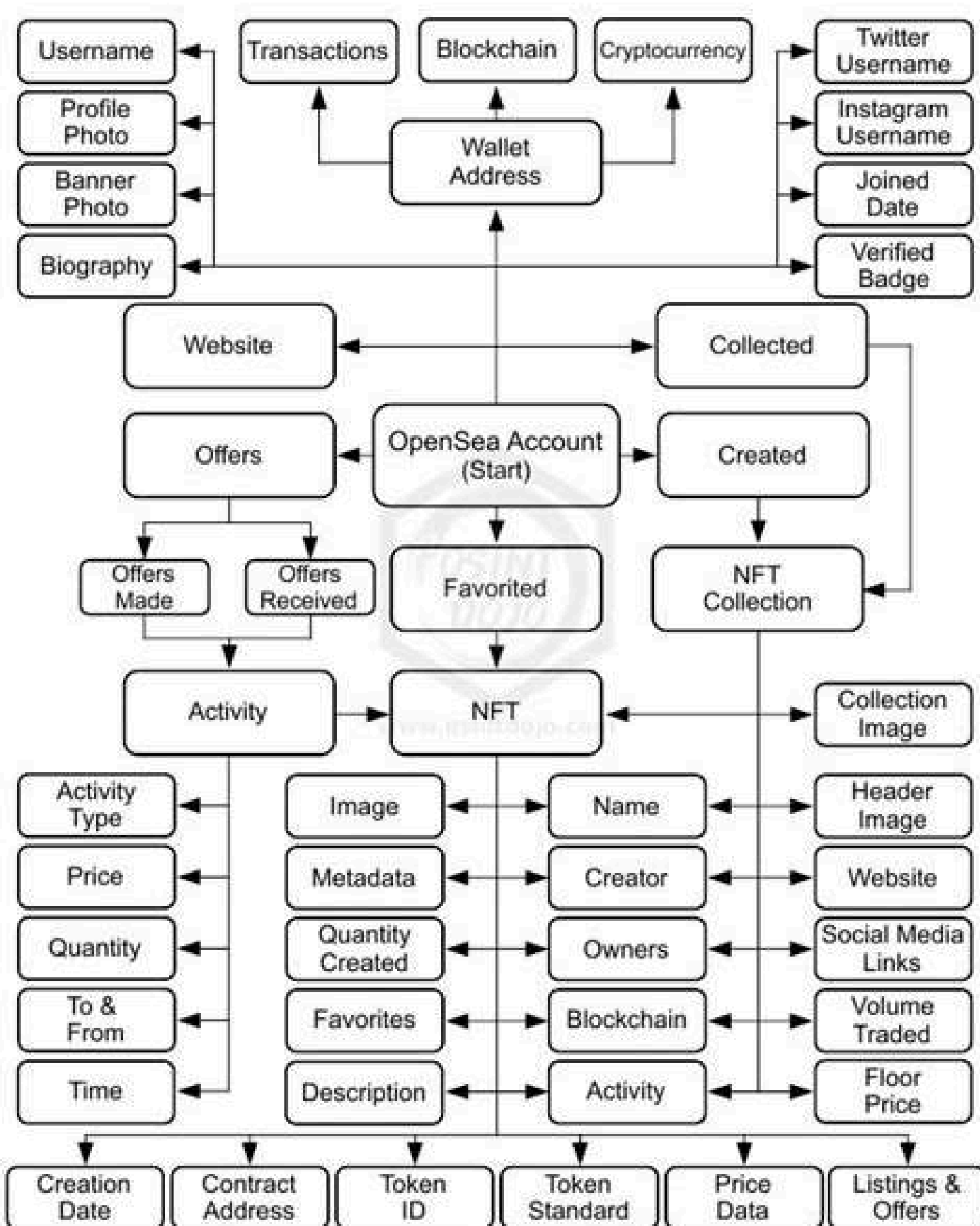


OpenSea Osint

- Explains OpenSea OSINT, focused on NFT transactions and wallet tracking.
- Discusses how blockchain transactions on OpenSea can be traced.
- Covers tools used for analyzing NFT ownership patterns.
- Suggests strategies to protect digital assets from OSINT investigations.

11. OpenSea OSINT

- Tools:
 - NFTScamAlert – Detects scam wallets.
 - Etherscan – Tracks Ethereum transactions.
- Exploits:
 - Fake NFT listings trick buyers.
- News:
 - 2023: OpenSea lost \$1.7M in NFT phishing attack.



Instagram Osint

- Introduces Instagram OSINT, focusing on location tracking and hashtag analysis.
- Discusses how metadata from images can reveal sensitive information.
- Highlights third-party tools for extracting Instagram insights.
- Suggests securing Instagram profiles to prevent data leakage.

4. Instagram OSINT

Tools:

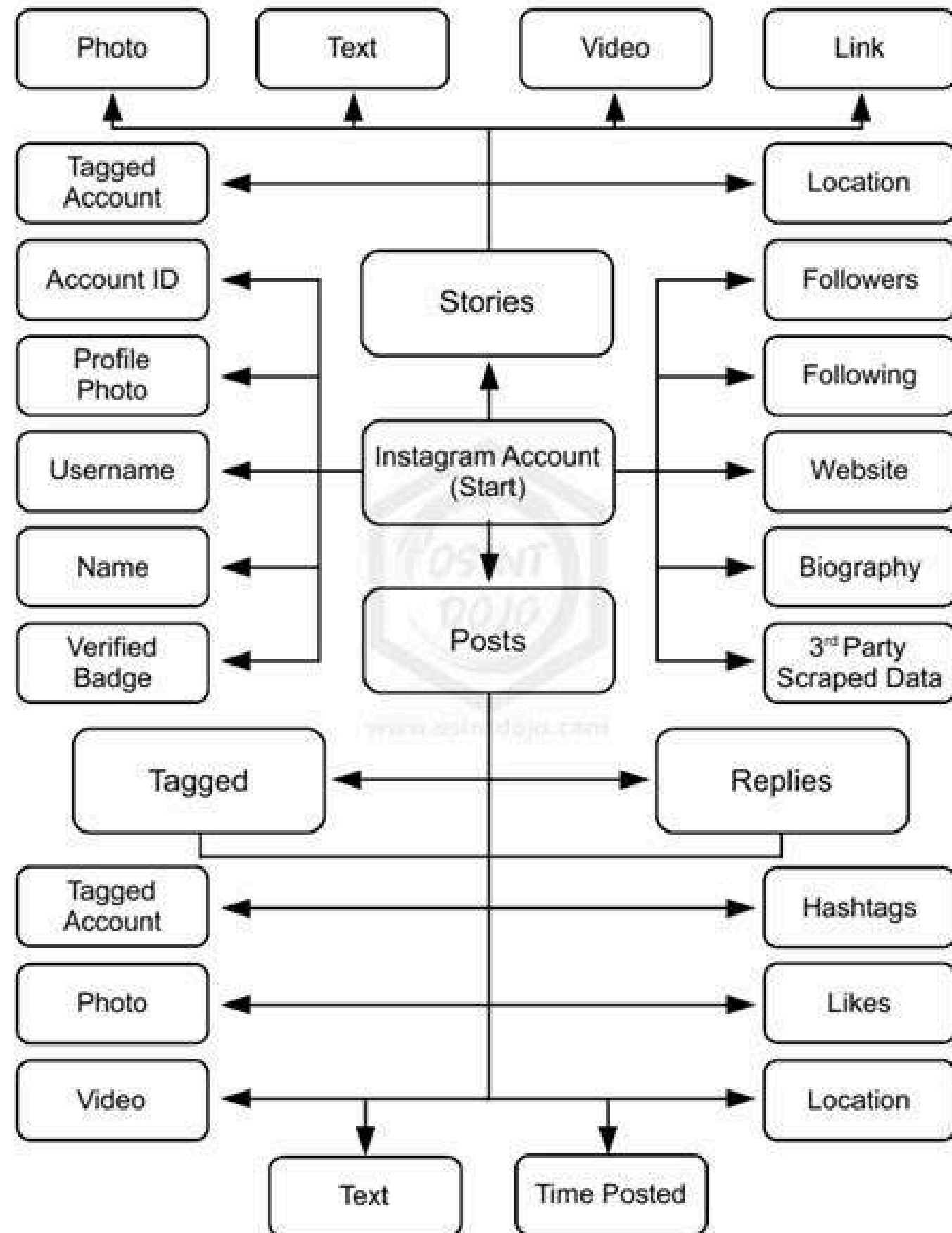
- Instaloader – Downloads images, metadata, and geolocation.
- Sowdust – Extracts Instagram insights.
- EagleEye – Identifies profiles via facial recognition.

Exploits:

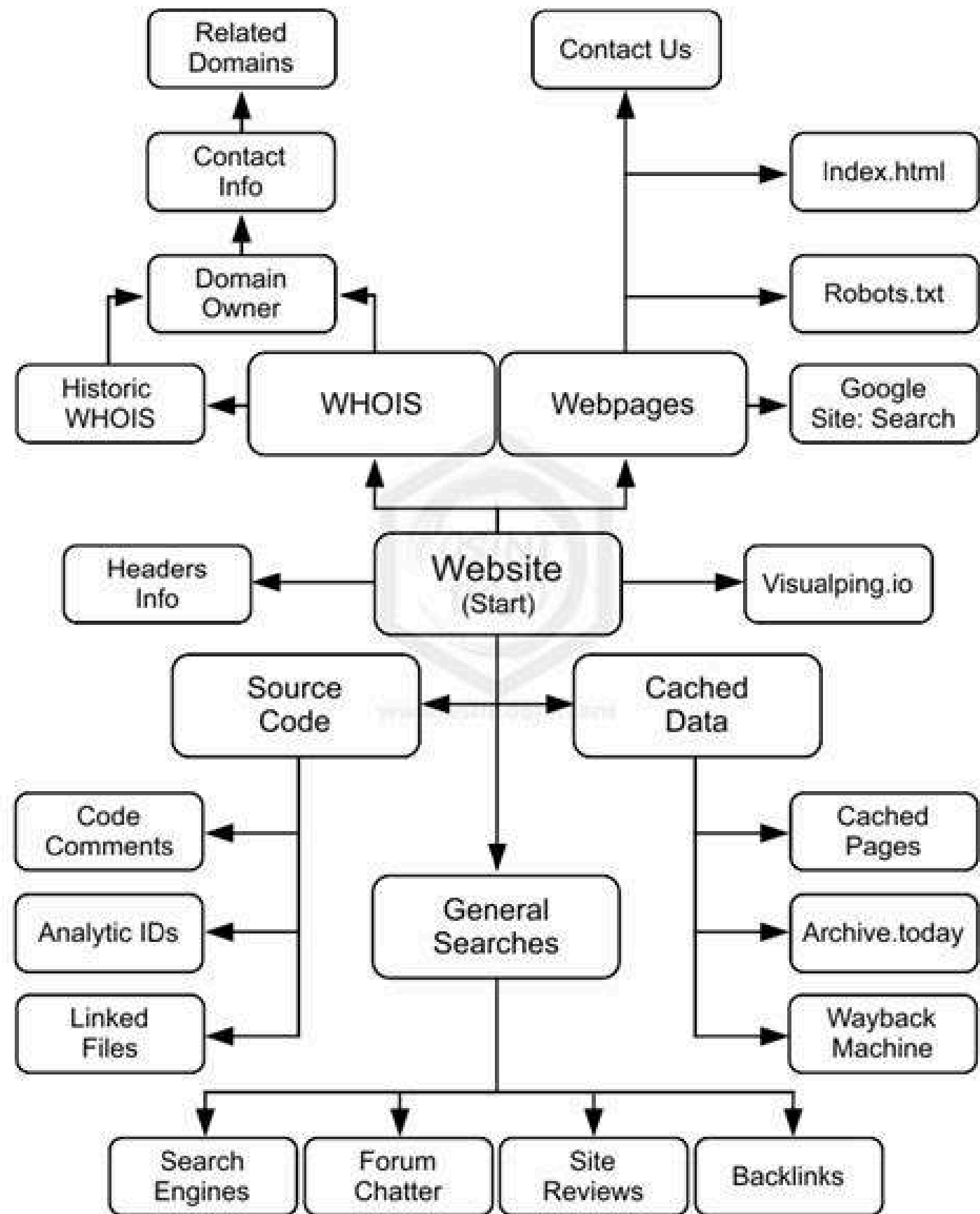
- Metadata in images exposes GPS coordinates.
- Hashtag analysis reveals user trends.

News:

- 2023: Instagram fined €405M for violating child privacy laws.



Website Osint

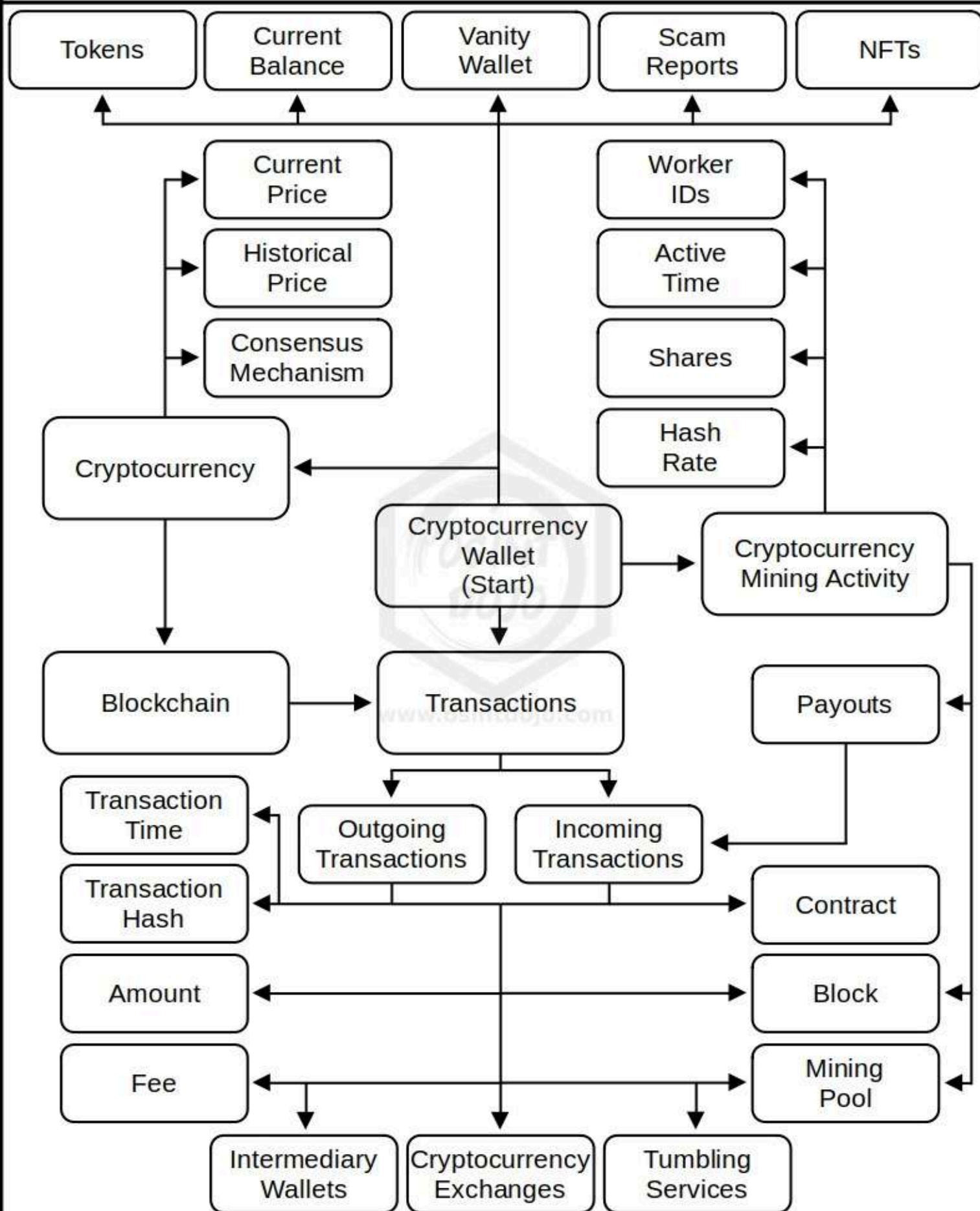


- Explores Website OSINT, including domain lookup and analytics tracking.
- Covers WHOIS data analysis and website fingerprinting.
 - Highlights how attackers analyze websites for vulnerabilities.
- Suggests securing websites against OSINT-based attacks.

Website & IP OSINT

9. Website OSINT

- Tools:
 - Shodan – Scans for open ports and vulnerabilities.
 - BuiltWith – Identifies website technologies.
 - Wayback Machine – Retrieves deleted pages.
- Exploits:
 - WHOIS data exposes personal info.
- News:
 - 2023: ICANN updated WHOIS privacy rules.



Cryptocurrency Osint

- Introduces Cryptocurrency OSINT, covering blockchain analysis.
- Discusses tracking transactions on public ledgers.
- Highlights privacy concerns related to transparent financial records.
- Suggests using mixing services and privacy coins for enhanced anonymity.

💰 Cryptocurrency OSINT

8. Crypto OSINT

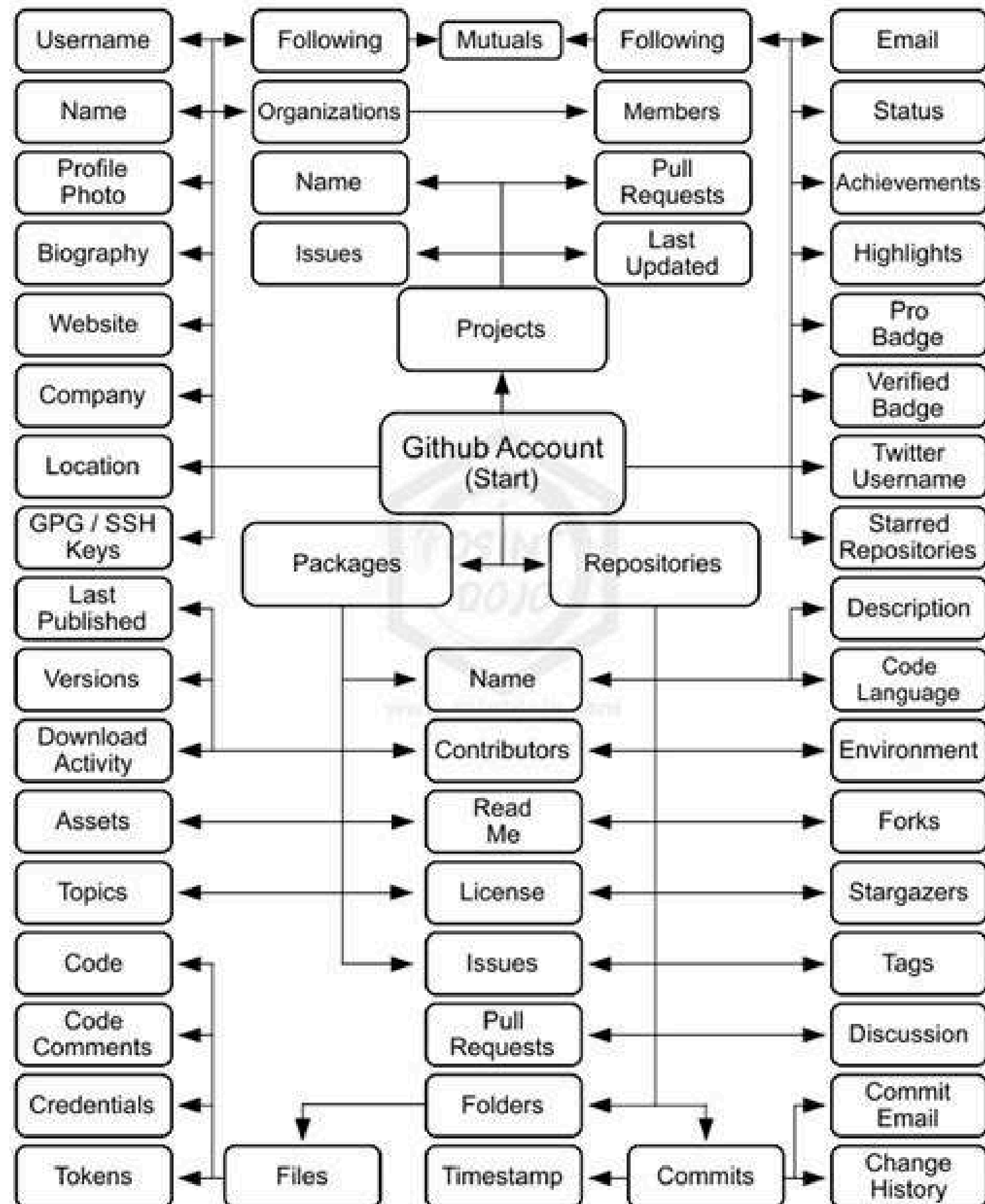
- Tools:
 - Blockchain Explorer – Tracks Bitcoin transactions.
 - CipherTrace – Identifies illicit cryptocurrency flows.
- Exploits:
 - Wallet reuse allows deanonymization.
- News:
 - 2023: Chainalysis uncovered \$20B in illicit crypto transactions.

Github Osint

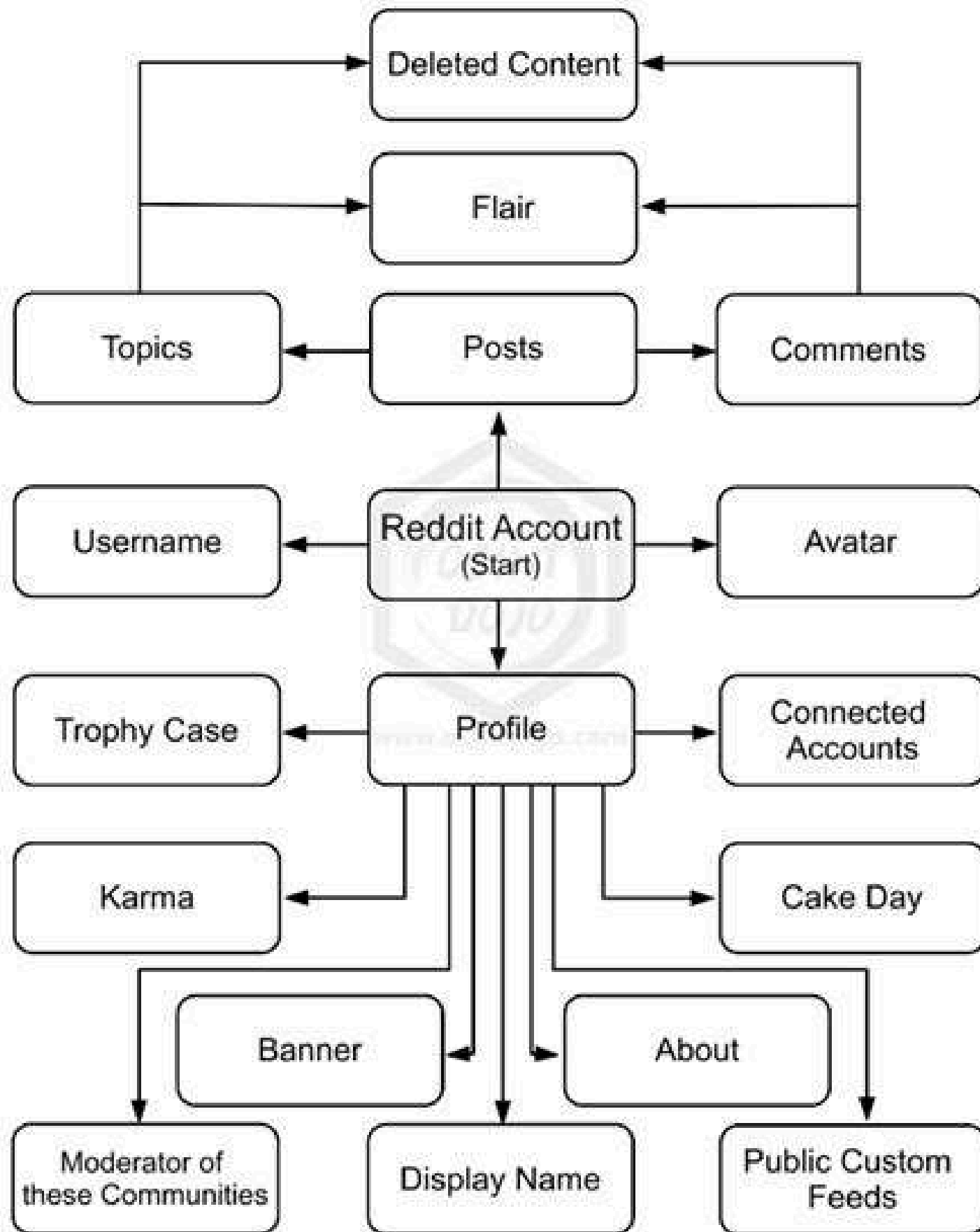
- Introduces GitHub OSINT, which focuses on tracking open-source contributions.
- Discusses how repositories reveal developer activity and credentials.
- Highlights security concerns around exposed API keys in GitHub repositories.
- Suggests securing GitHub repositories to prevent OSINT exploitation.

12. GitHub OSINT

- Tools:
 - Gitleaks – Finds leaked API keys.
 - RepoHunt – Tracks developer activities.
- Exploits:
 - Hardcoded credentials expose systems.
- News:
 - 2023: GitHub introduced secret scanning alerts.



Reddit Account

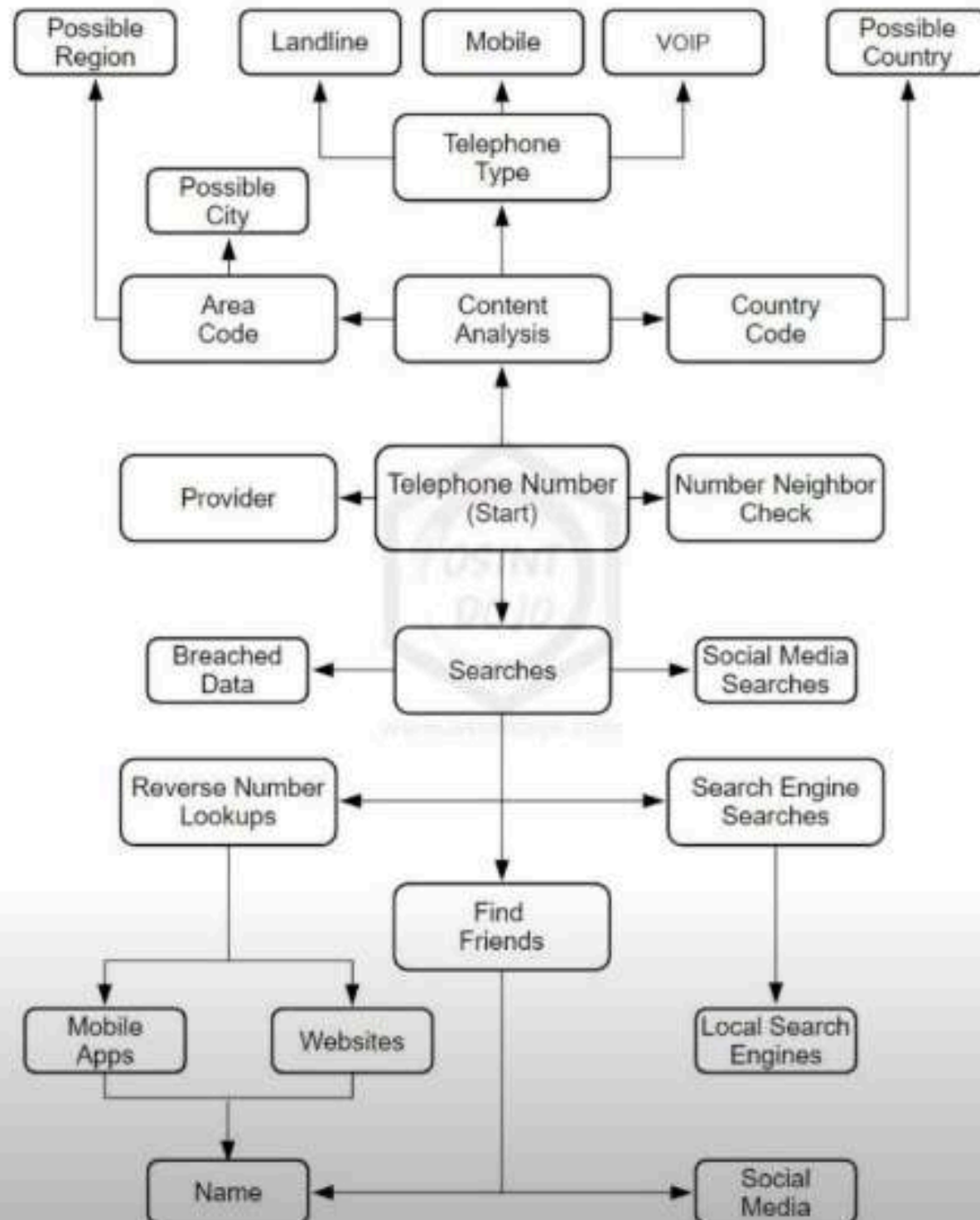


- Introduces Reddit OSINT, covering user activity tracking.
- Discusses subreddit participation as a source of intelligence.
- Highlights risks of exposed historical posts revealing sensitive information.
- Suggests securing Reddit accounts and using anonymous browsing.

13. Reddit OSINT

- Tools:
 - Pushshift – Retrieves deleted comments.
 - RedditScraper – Collects post history.
- Exploits:
 - Old posts reveal identity links.
- News:
 - 2023: Reddit leaked user DMs in a security incident.

Phone OSINT Attack Surface

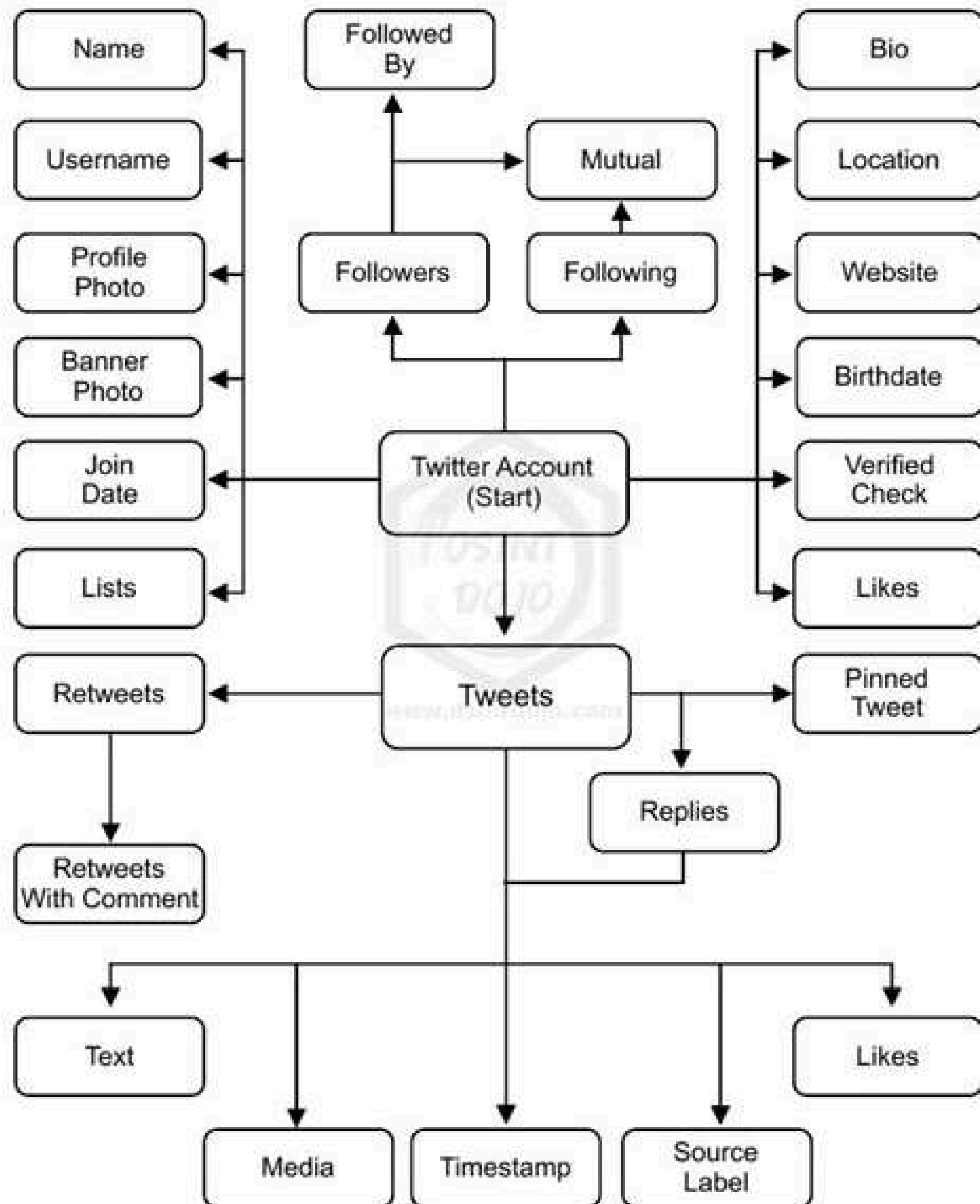


Phone Osint

- Discusses Phone OSINT and how mobile numbers can be tracked.
- Covers call detail records, carrier lookup, and geolocation tracking.
- Highlights how scammers use phone OSINT for fraud.
- Recommends securing mobile numbers through privacy settings.

7. Phone OSINT

- Tools:
 - PhoneInfoga – Identifies carrier and country of phone numbers.
 - TrueCaller OSINT – Scrapes names linked to numbers.
- Exploits:
 - SIM swap attacks expose banking details.
- News:
 - 2023: T-Mobile suffered a SIM swap breach affecting 37M customers.

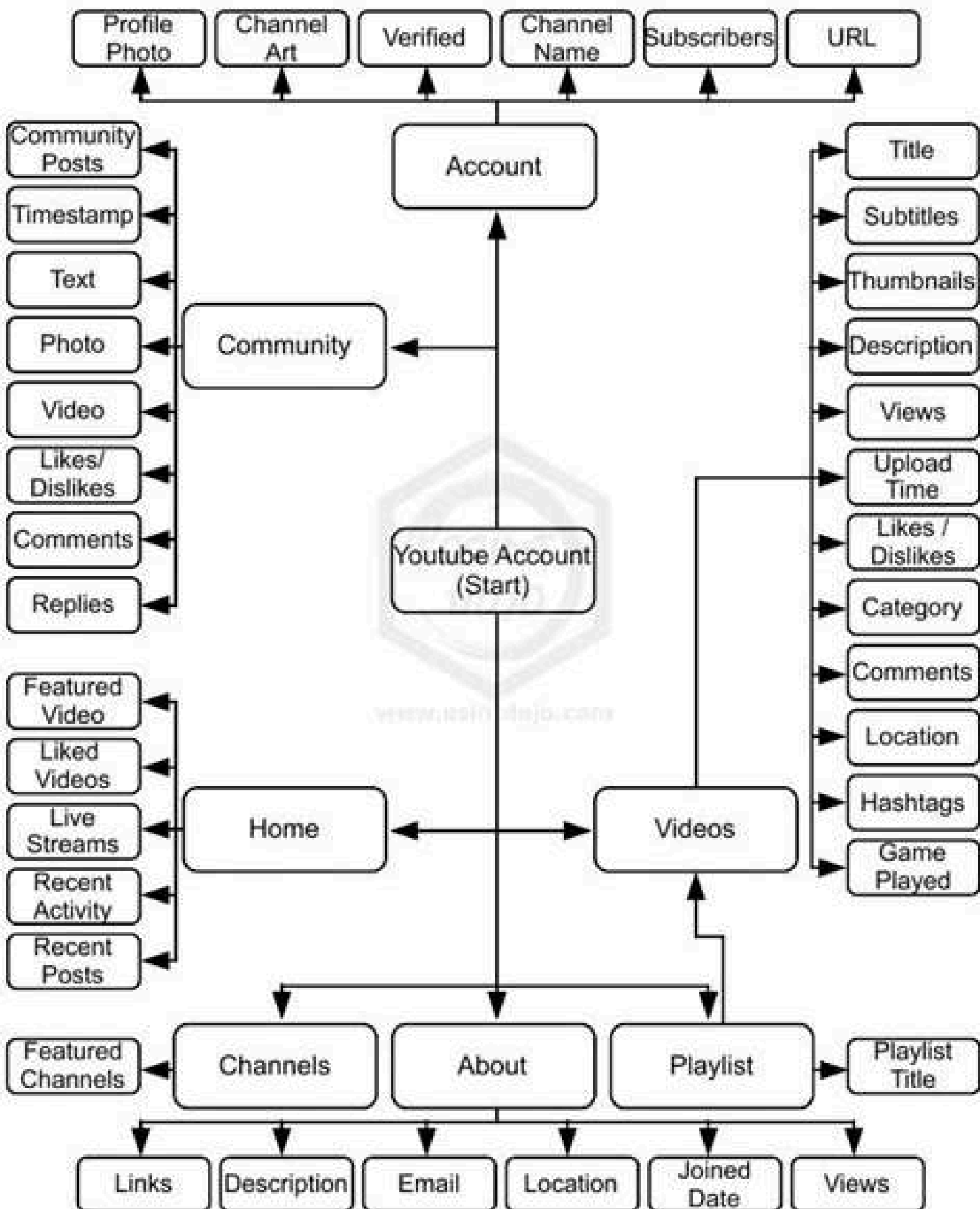


Twitter Osint

- Brevity and Character Limit
- Asymmetric Following and Public Engagement
- Hashtags and Viral Dynamics
- Advanced Features for Creators and Brands

5. Twitter OSINT

- Tools:
 - Twint – Scrapes Twitter data without API limits.
 - TweetBeaver – OSINT automation for Twitter.
- Exploits:
 - Deleted tweets still accessible via third-party archives.
- News:
 - 2023: Twitter API leaks exposed 200M user emails.



Youtube Osint

- Discusses YouTube OSINT and how video metadata can be analyzed.
- Covers techniques for tracking upload timestamps and geolocation.
- Explains how video content reveals user habits and locations.
- Suggests ways to anonymize video uploads to prevent OSINT tracking.

YouTube OSINT Tools – YouTube Metadata Tool, InVID, YouTube Data API for tracking video metadata, timestamps, and geolocation.

Person Attack Surface for OSINT Investigations

```
graph TD
    PersonStart[Person (Start)] --> Vehicle[Vehicle]
    PersonStart --> FriendsFamily[Friends / Family]
    PersonStart --> OnlinePresence[Online Presence]
    PersonStart --> GangAffiliation[Gang Affiliation]

    Vehicle --> FrequentLocations[Frequent Locations]
    Vehicle --> EventsAppointments[Events / Appointments]

    FriendsFamily --> OtherIRLAttributes[Other IRL Attributes]
    FriendsFamily --> OnlinePresence

    OnlinePresence --> UserAgents[User Agents]
    OnlinePresence --> IPISP[IP / ISP]

    GangAffiliation --> UserAgents
    GangAffiliation --> IPISP

    PersonStart --> YearMakeModel[Year / Make / Model]
    PersonStart --> Color[Color]
    PersonStart --> ModsDamage[Mods or Damage]
    PersonStart --> LicensePlate[License Plate]
    PersonStart --> VIN[VIN]

    PersonStart --> Work[Work]
    PersonStart --> HangOutSpots[Hang-Out Spots]
    PersonStart --> Home[Home]
    PersonStart --> School[School]

    Work --> BossCoworkers[Boss / Coworkers]
    Work --> NearbySexOffenders[Nearby Sex Offenders]
    Work --> OtherLocalThreats[Other Local Threats]
    Work --> DirectionTraveling[Direction Traveling]
    Work --> Classmates[Classmates]

    HangOutSpots --> BossCoworkers
    HangOutSpots --> NearbySexOffenders
    HangOutSpots --> OtherLocalThreats
    HangOutSpots --> DirectionTraveling
    HangOutSpots --> Classmates

    Home --> BossCoworkers
    Home --> NearbySexOffenders
    Home --> OtherLocalThreats
    Home --> DirectionTraveling
    Home --> Classmates

    School --> BossCoworkers
    School --> NearbySexOffenders
    School --> OtherLocalThreats
    School --> DirectionTraveling
    School --> Classmates

    PersonStart --> ClothingJewelry[Clothing / Jewelry]
    PersonStart --> Mood[Mood]
    PersonStart --> Weather[Weather]
    PersonStart --> LocationLastSeen[Location Last Seen]
    PersonStart --> LastSeenWith[Last Seen With]

    ClothingJewelry --> DateLastSeen[Date Last Seen]
    Mood --> DateLastSeen
    Weather --> DateLastSeen
    LocationLastSeen --> DateLastSeen
    LastSeenWith --> DateLastSeen

    DateLastSeen --> Appearance[Appearance]

    PersonStart --> GenderIdentity[Gender Identity]
    PersonStart --> MedicalConditions[Medical Conditions]
    PersonStart --> DateOfBirth[Date of Birth]
    PersonStart --> PlaceOfBirth[Place of Birth]
    PersonStart --> Habits[Habits]
    PersonStart --> NamesNicknames[Names / Nicknames]

    DateOfBirth --> PlaceOfBirth

    PersonStart --> ElectronicDevices[Electronic Devices]
    PersonStart --> PhoneNumbers[Phone Numbers]

    ElectronicDevices --> TelephoneCarrier[Telephone Carrier]
    PhoneNumbers --> TelephoneCarrier

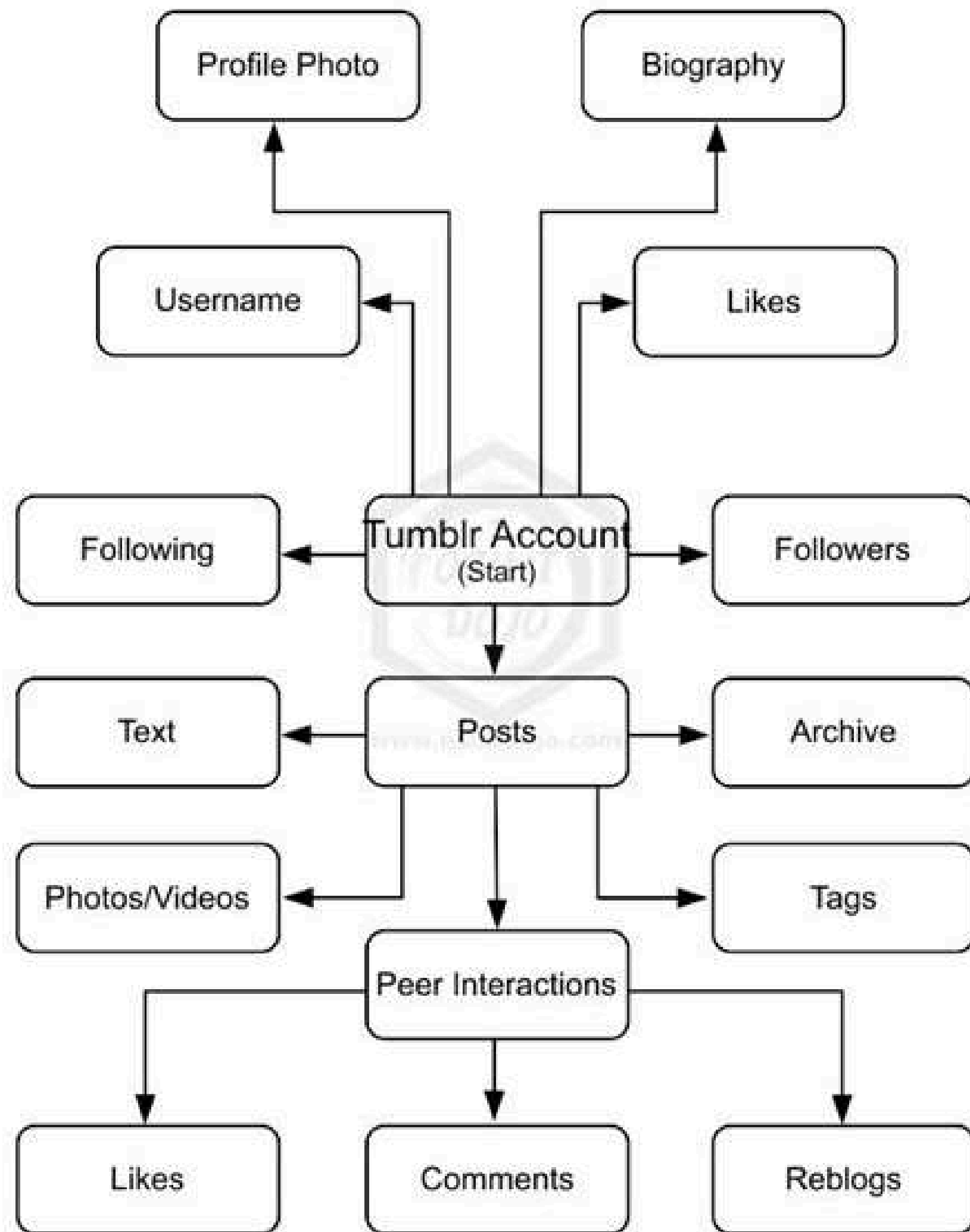
    PersonStart --> Citizenship[Citizenship]

    OnlinePresence --> Usernames[Usernames]
    OnlinePresence --> Emails[Emails]
    OnlinePresence --> SocialMedia[Social Media]
    OnlinePresence --> PersonalWebsites[Personal Websites]
    OnlinePresence --> PersonSearches[Person Searches]
    OnlinePresence --> ArticlesBlogs[Articles / Blogs]
    OnlinePresence --> Gaming[Gaming]
```

Person Osint

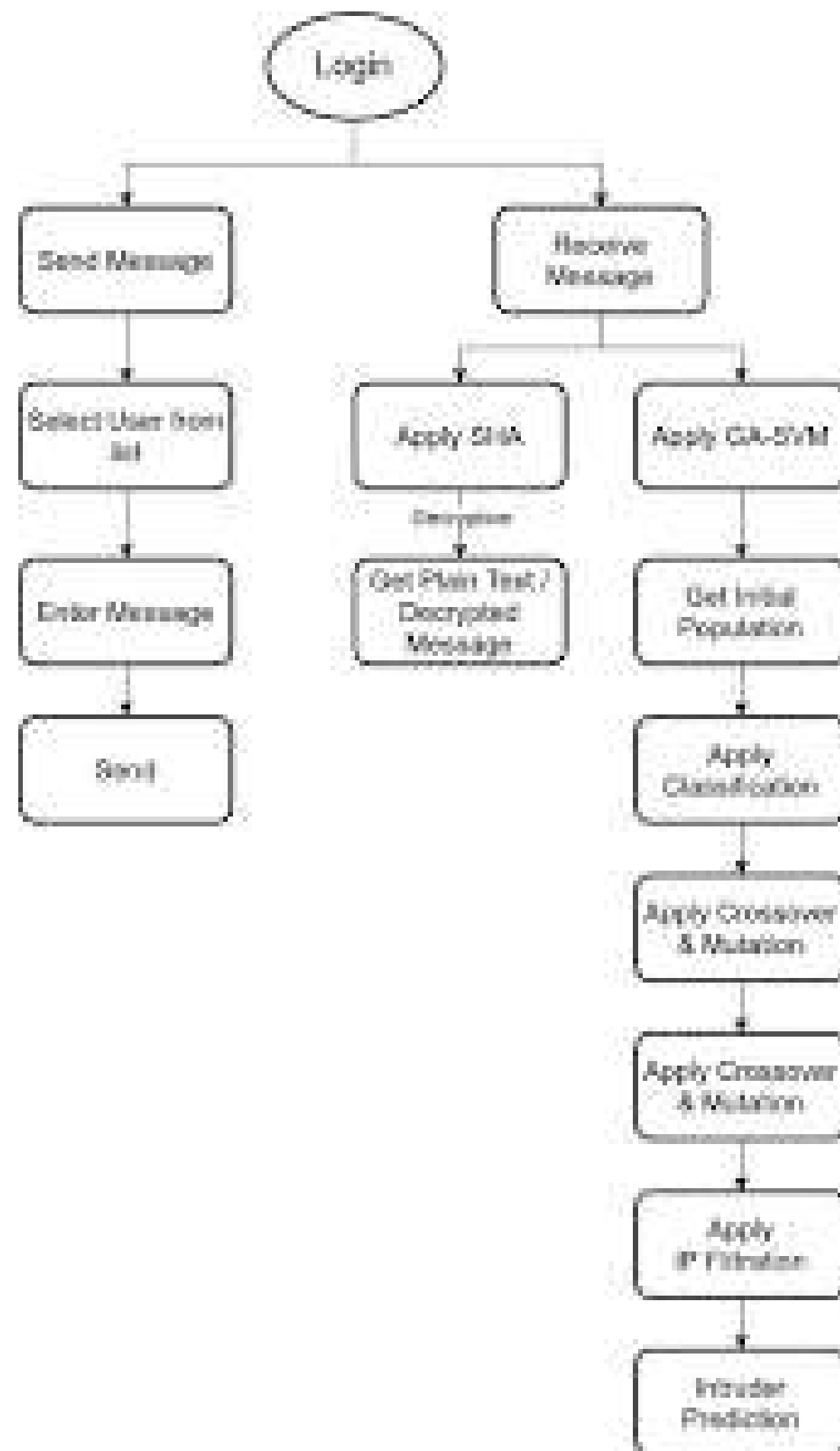
- **Explores Person OSINT, which involves gathering data on individuals.**
- **Covers search engine techniques, social media footprint tracking, and database searches.**
- **Highlights risks of personal data leaks through public records.**
- **Suggests privacy best practices for securing personal information.**

Person OSINT Tools – Sherlock, Maigret, NameCheckUp for finding usernames and profiles across platforms.



Tumblr Osint

- Covers Tumblr OSINT, emphasizing blog activity monitoring.
- Discusses how Tumblr posts and comments can be used for intelligence gathering.
- Highlights risks of exposing personal data through old Tumblr posts.
- Recommends securing Tumblr accounts to minimize OSINT exposure.



Login Osint

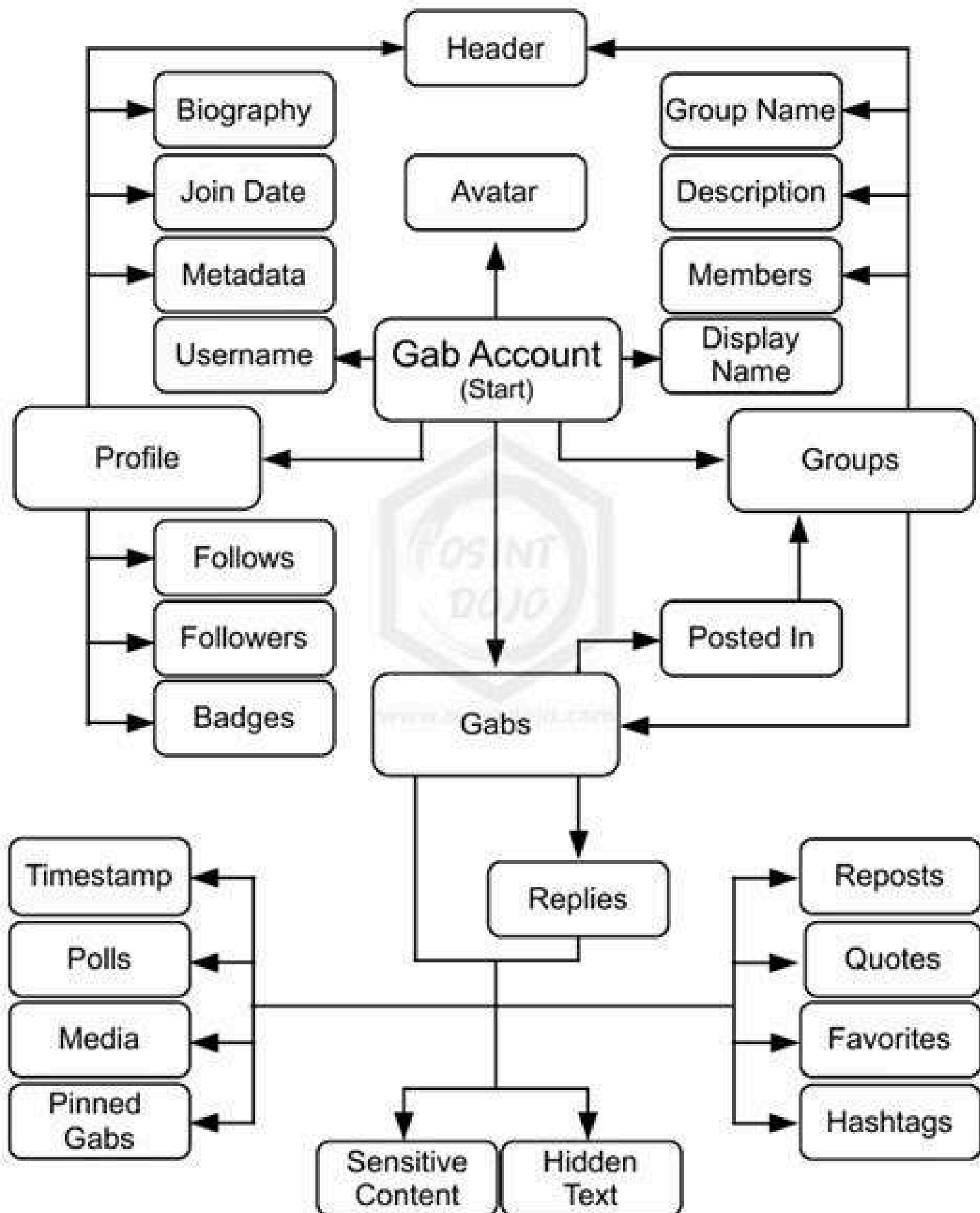
- Covers Login OSINT, focusing on tracking login credentials and breaches.
- Discusses analyzing leaked credentials from data breaches.
- Highlights risks of password reuse across multiple platforms.
- Suggests best practices for secure authentication.

Login OSINT Tools – Have I Been Pwned, Dehashed, and Snubase for tracking leaked credentials

Gab Osint

- Covers Gab OSINT, discussing how social media intelligence is extracted.
- Highlights how extremist groups use Gab for communication.
- Explains monitoring techniques for law enforcement.
- Suggests securing Gab accounts to limit OSINT exposure.

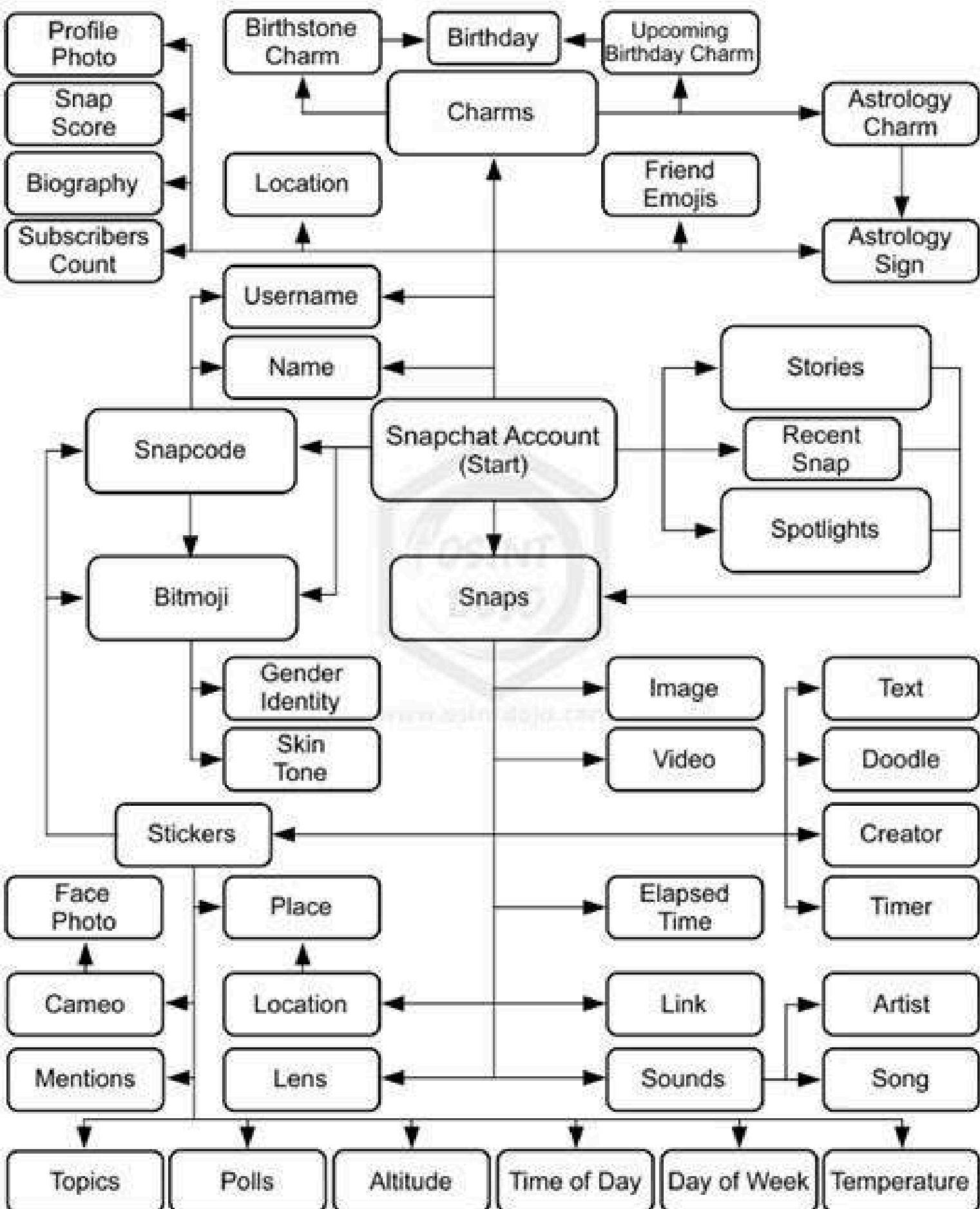
Gab OSINT Tools – Gab API monitoring, OSINT Framework for extremist tracking, and social network analysis.

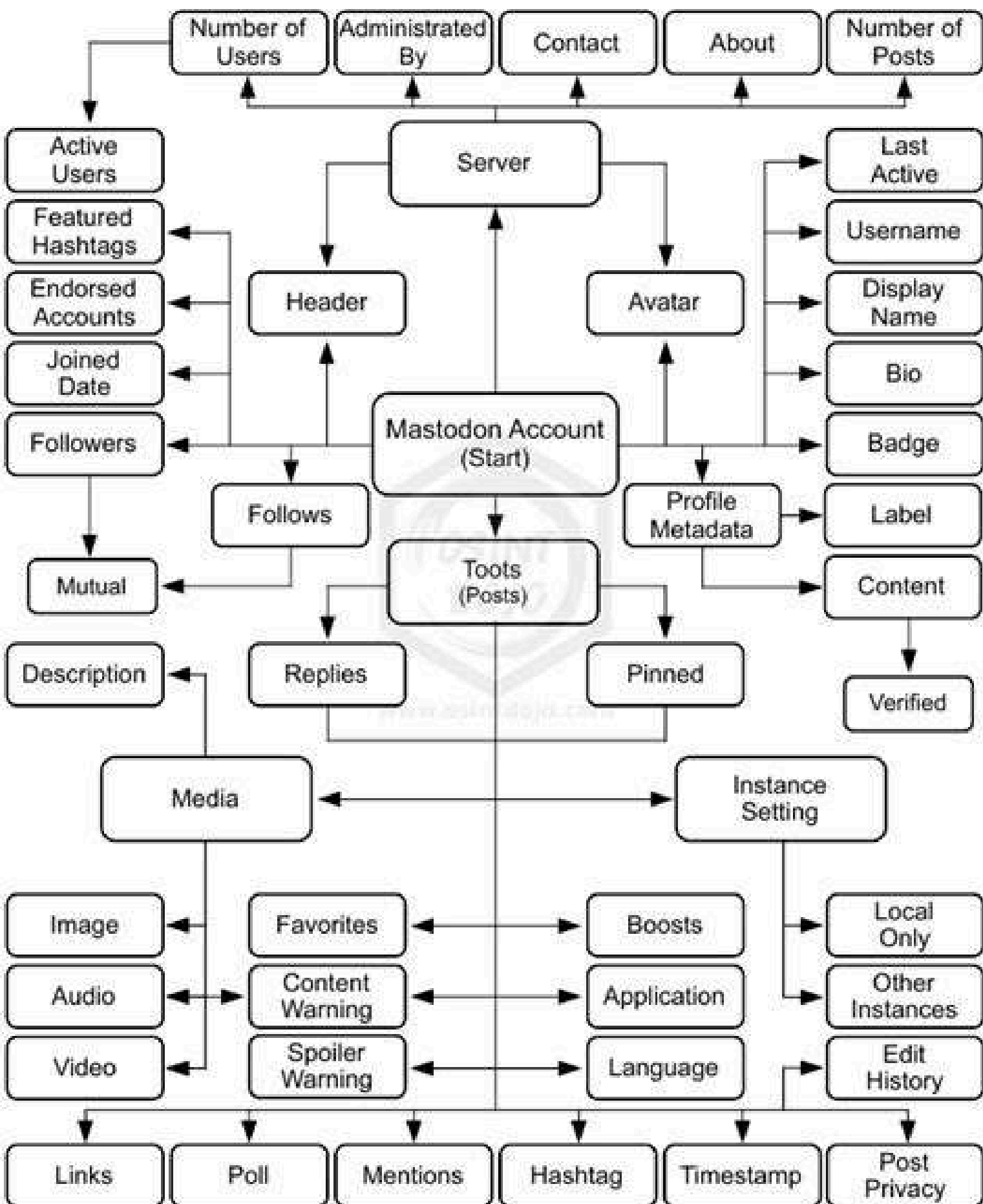


Snap Chat Osint

- Discusses Snapchat OSINT, focusing on location tracking via Snap Maps.
- Covers metadata extraction from Snapchat stories and images.
- Highlights risks of publicly shared snaps revealing personal data.
- Suggests securing Snapchat accounts to prevent OSINT tracking.

Snapchat OSINT Tools – Snap Map, ExifTool for metadata extraction, and forensic analysis tools.





Mastodon Account

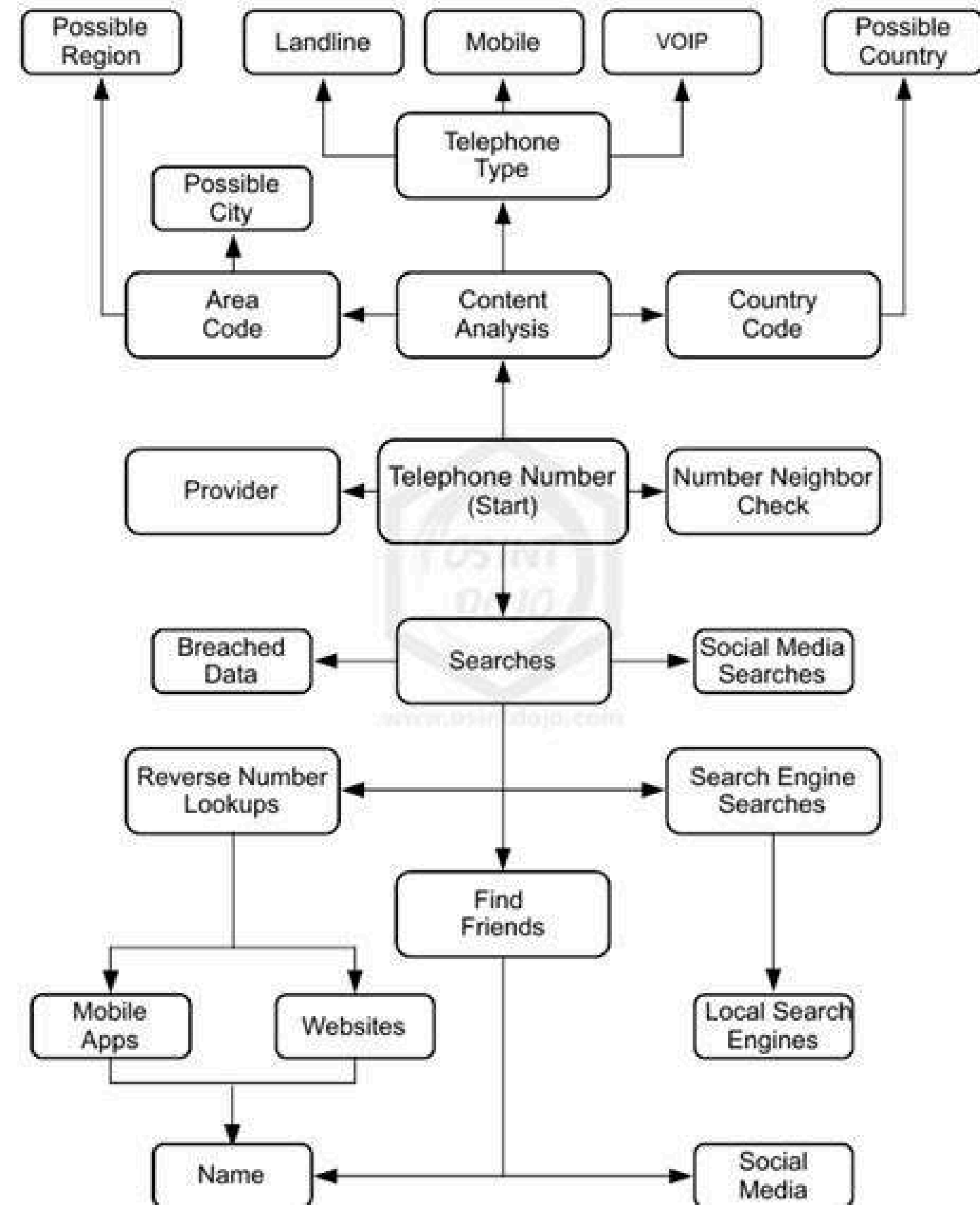
- Covers Mastodon OSINT, focusing on decentralized social media tracking.
- Discusses federated networks and user activity monitoring.
- Highlights privacy concerns associated with Mastodon's public posting.
- Suggests ways to maintain anonymity on Mastodon.

Mastodon OSINT Tools– Fediverse.tools, TheHarvester for federated social media tracking.

Telephone Osint

- Covers Telephone OSINT, analyzing call records and VOIP data.
- Discusses phone number intelligence gathering techniques.
- Highlights risks of data leaks from telecom providers.
- Suggests securing phone communications from OSINT tracking.

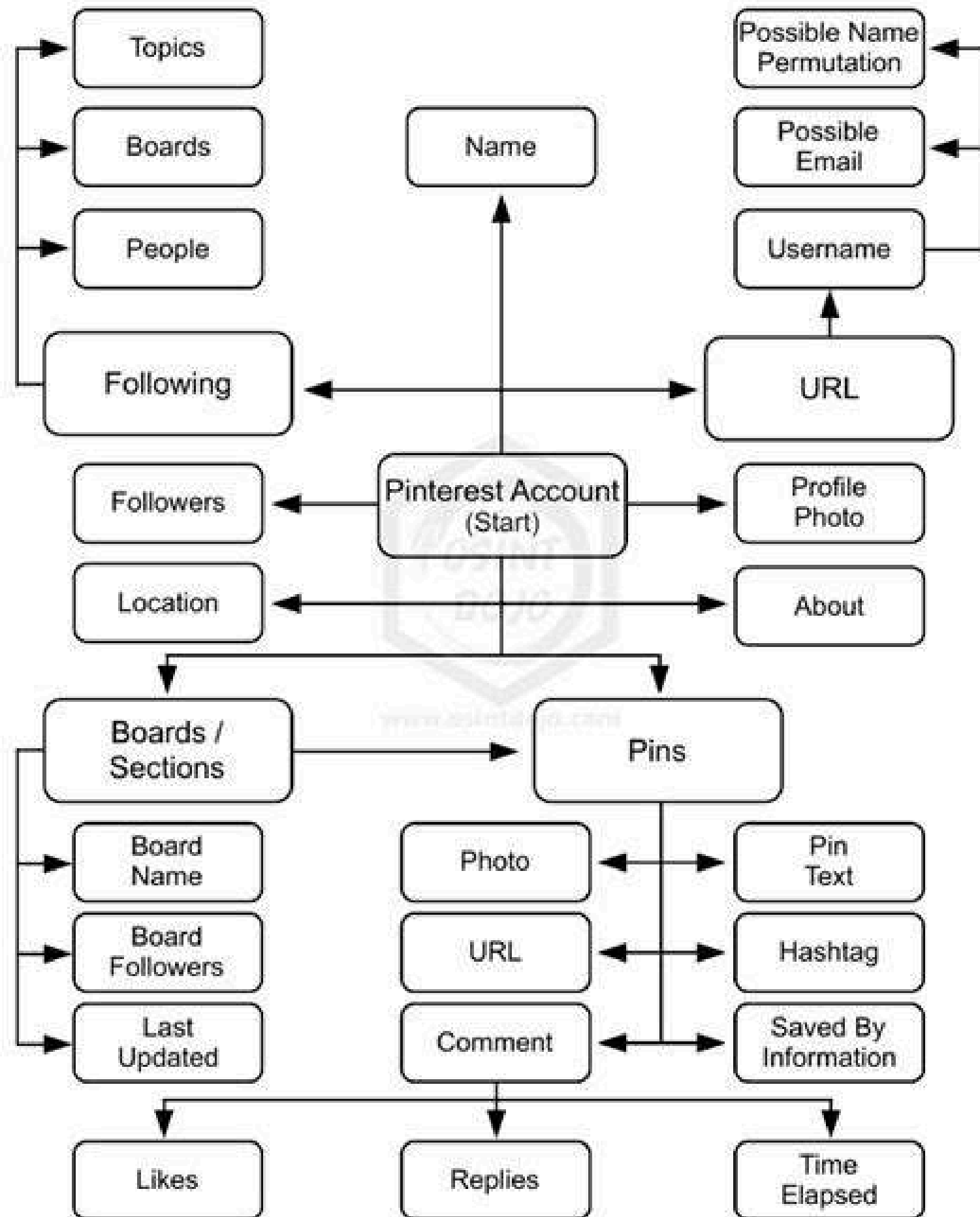
Telephone OSINT Tools – Truecaller, PhoneInfoga, NumVerify for call record analysis and telecom data leaks.

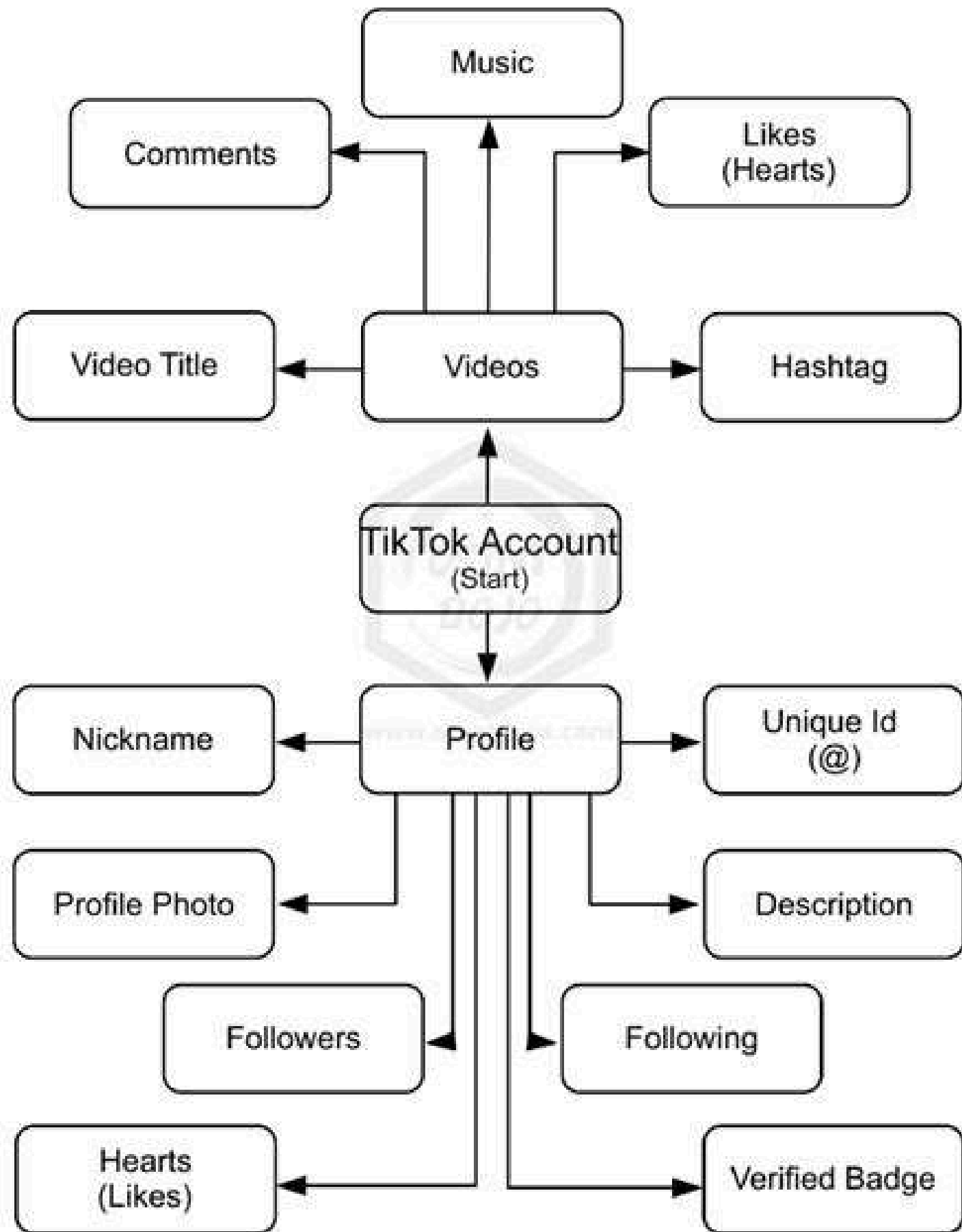


Pinterest Osint

- Covers Pinterest OSINT, focusing on tracking user interests and trends.
- Discusses how pinned content reveals user behavior.
- Highlights risks of metadata exposure in Pinterest images.
- Suggests ways to limit OSINT exposure on Pinterest.

Pinterest OSINT Tools– Pinsearch, Image Reverse Search for tracking image metadata.

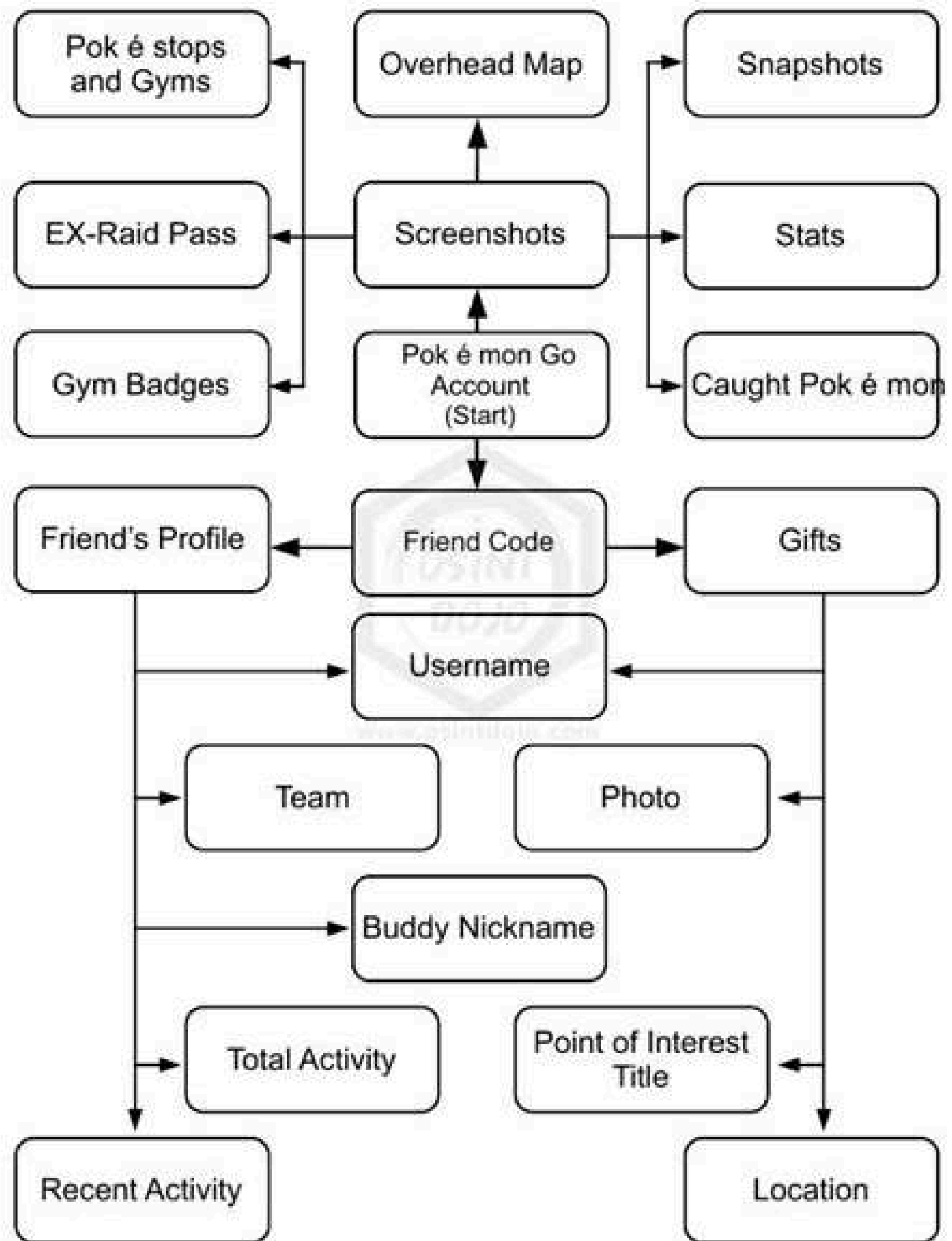




TikTok Osint

- Explores TikTok OSINT, focusing on tracking video metadata.
- Discusses how TikTok's algorithm exposes user activity.
- Highlights security concerns related to data collection.
- Suggests securing TikTok accounts to prevent tracking.

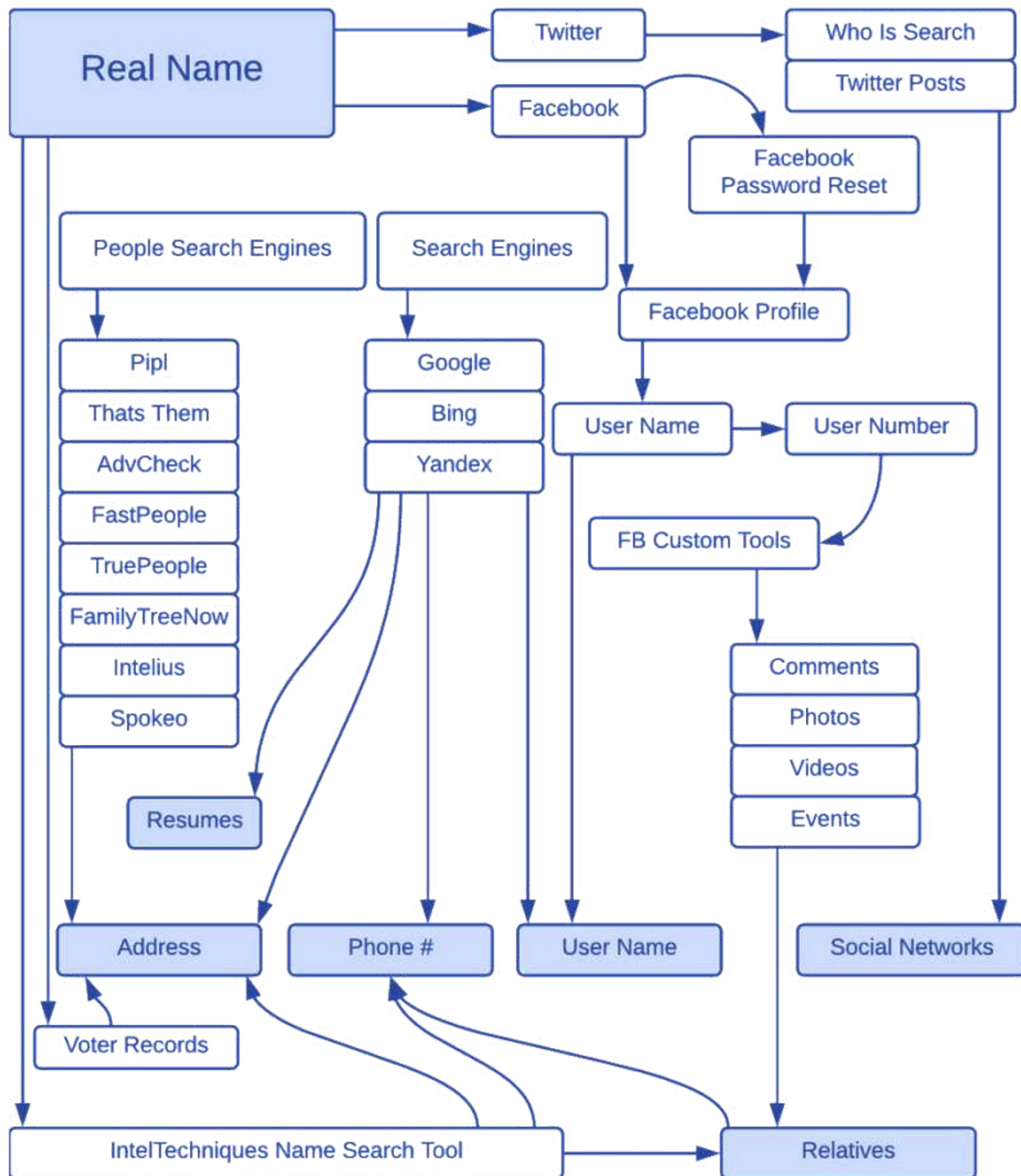
TikTok OSINT – OSINT Techniques, ExifTool, TikTok API monitoring for tracking user activities.



Pokemon Go Osint

- Discusses Pokémon Go OSINT, focusing on location tracking.
- Highlights risks of GPS-based gaming apps exposing personal movement patterns.
- Explains how attackers use Pokémon Go activity logs for intelligence.
- Suggests securing location settings to prevent tracking.

Pokémon Go OSINT Tools – PoGoMap, GPS Spoofing detection tools, location tracking via Pokémon Go logs.

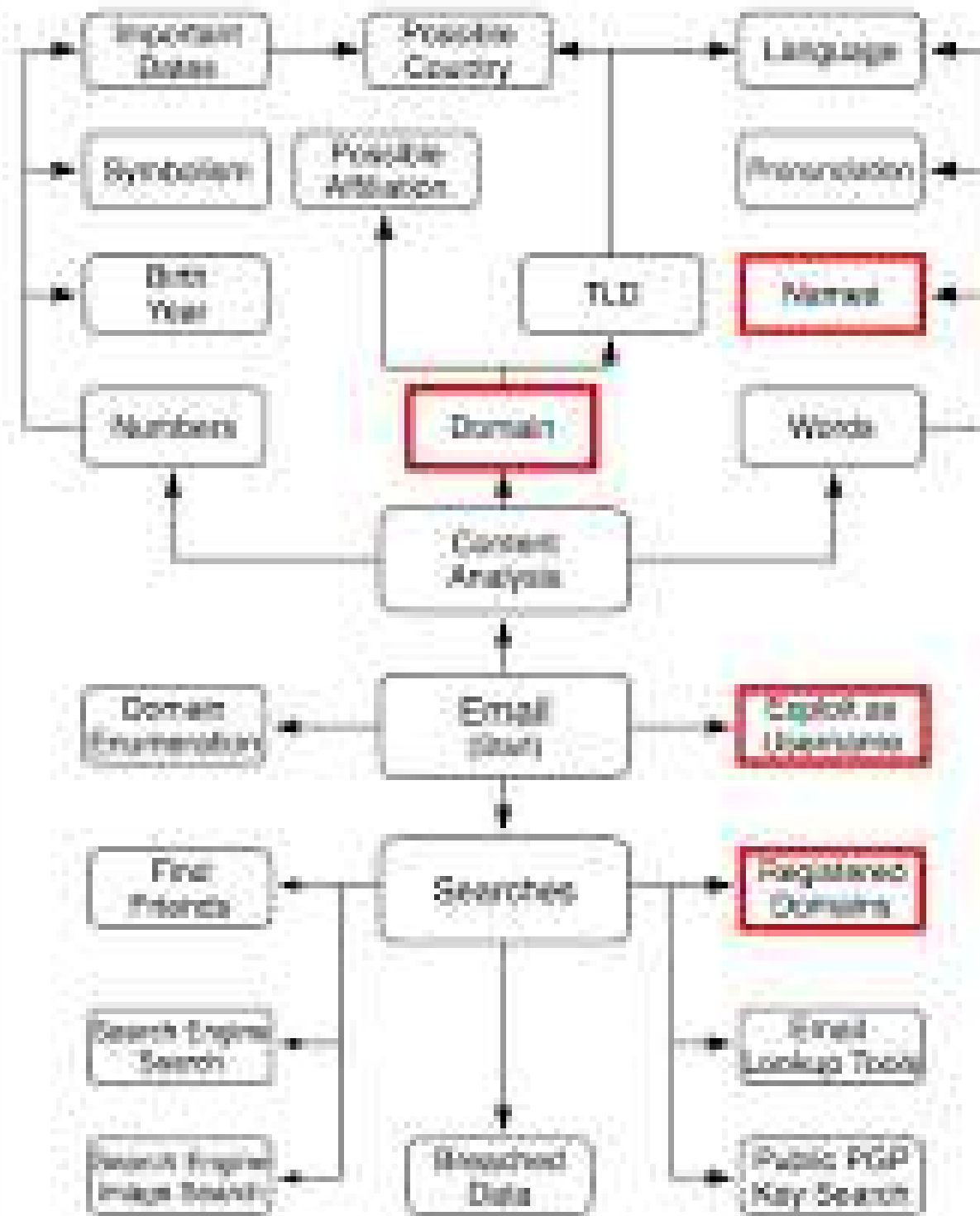


Real Name Osint

- Introduces Real Name OSINT, covering how identity data is tracked.
- Discusses methods to find real names associated with online personas.
- Highlights identity theft risks from exposed real-name data.
- Suggests securing personal identity online.

Real Name OSINT Tools– Maltego, Pipl, Spokeo for identity searches.

Email OSINT Attack Surface



Email Osint

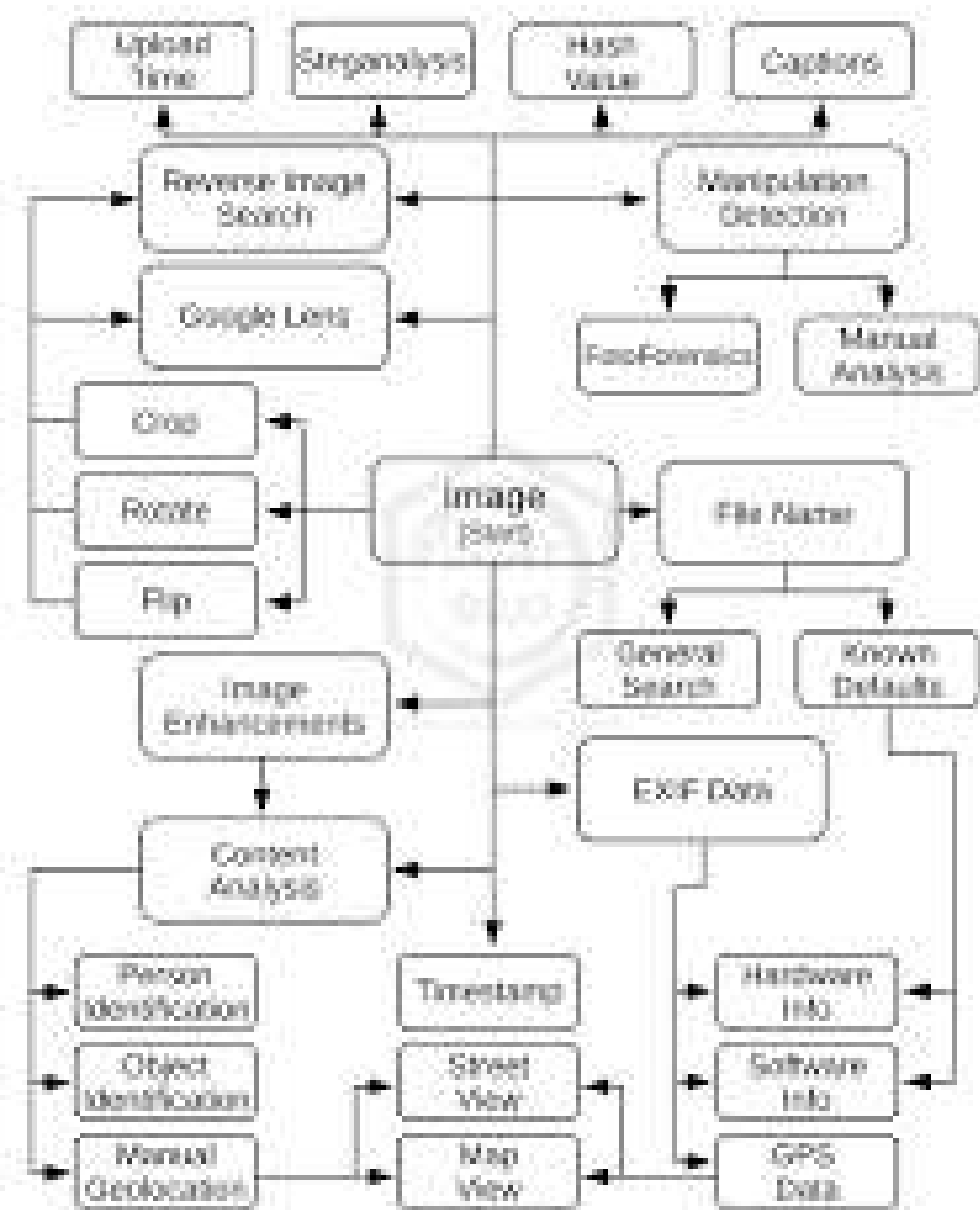
- Threat Detection and Prevention
- Investigations and Incident Response
- Compliance and Risk Management
- Cybersecurity Intelligence Gathering

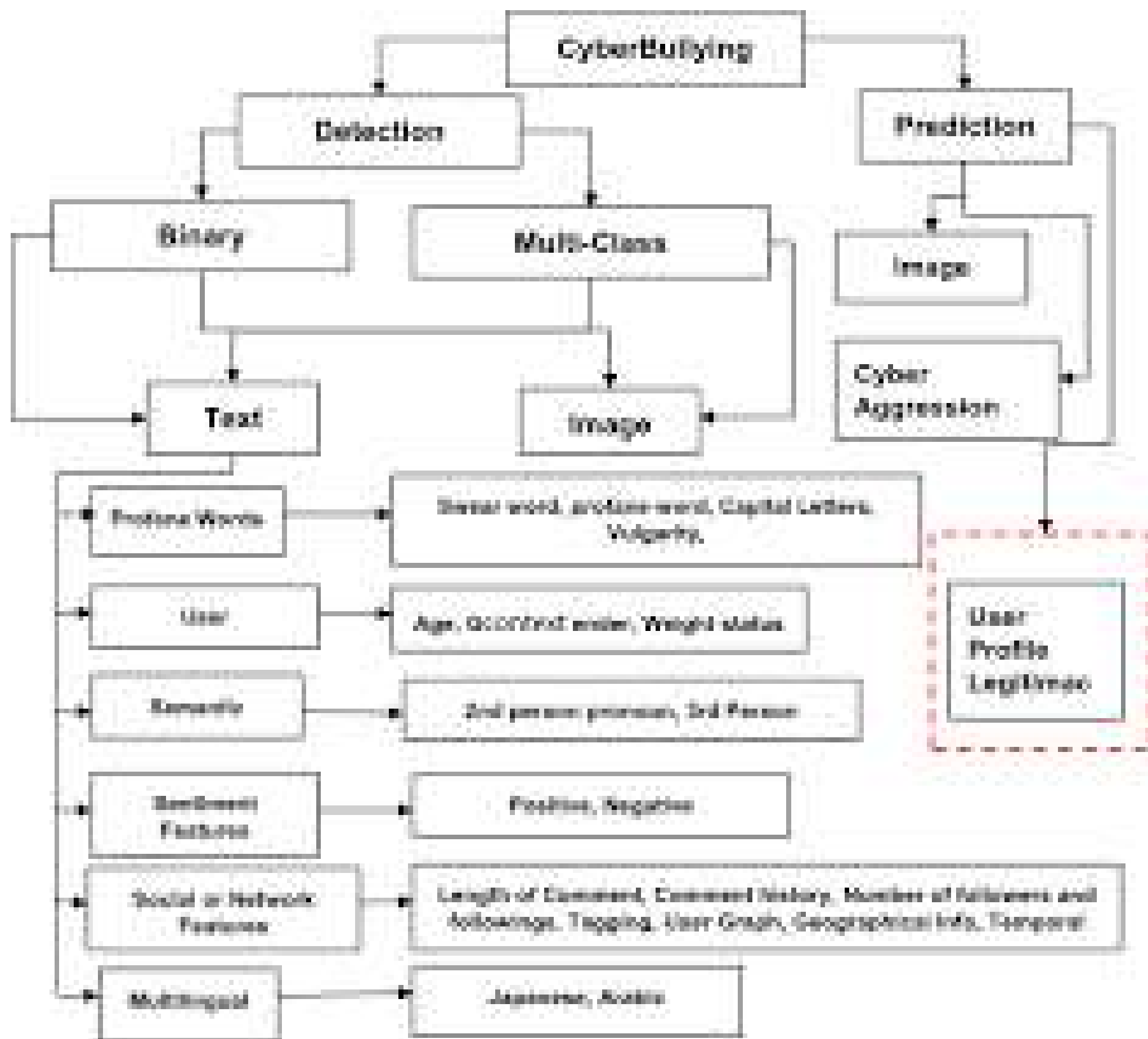
Email OSINT – Email-Header-Analyzer, Hunter.io, OSINT.email for email tracking and phishing detection.

Image Osint

- track individuals, locations, and objects
- Cybercrime & Fraud Investigations
- Journalism & Fact-Checking
- leaked sensitive images

Image OSINT – ExifTool, Google Lens, Forensically for metadata analysis and deepfake detection.





```
kali@kali: ~  
$ spiderfoot -i 127.0.0.1:8080
```

Activate Windows
Go to Settings to activate Windows.

To direct input to this VM, click inside or press Ctrl+G.



**Thank You
Very Much!**

Tools:-

@BreachHunter_Bot

@khoj

<https://teleteg.com/>

Google Earth Pro

<https://epieos.com/>

[https://linktr.ee/digisur
?utm_source=linktre...](https://linktr.ee/digisur?utm_source=linktre...)

