Open Source Intelligence

Presented by Shivam

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 | Take a Tour

Contribute | Blog

FAQ | 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

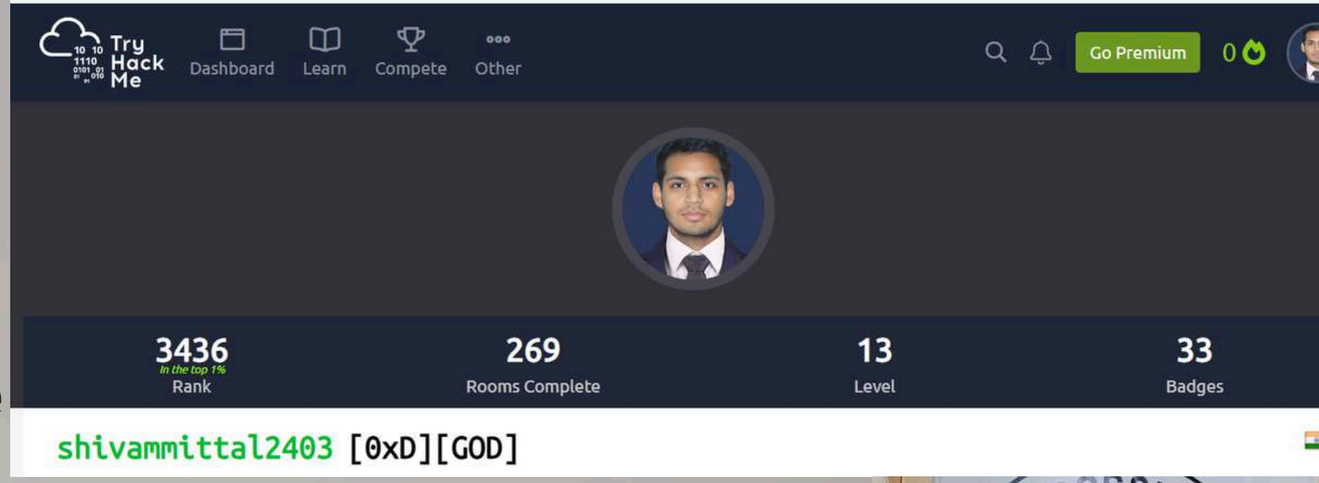
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	44 techniques	17 techniques	32 techniques	9 techniques	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)
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)
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration	Boot or Logon Autostart Execution (14)	Account Manipulation (5)	BITS Jobs	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture
Gather Victim Network	Compromise Infrastructure (6)			Boot or Logon		Build Image on Host		Cloud Infrastructure Discovery		Automated

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

minal

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

New | Save | Load | Windows | Search for a helper | Circular | Hierarchical | Radial | Force-Directed

ools

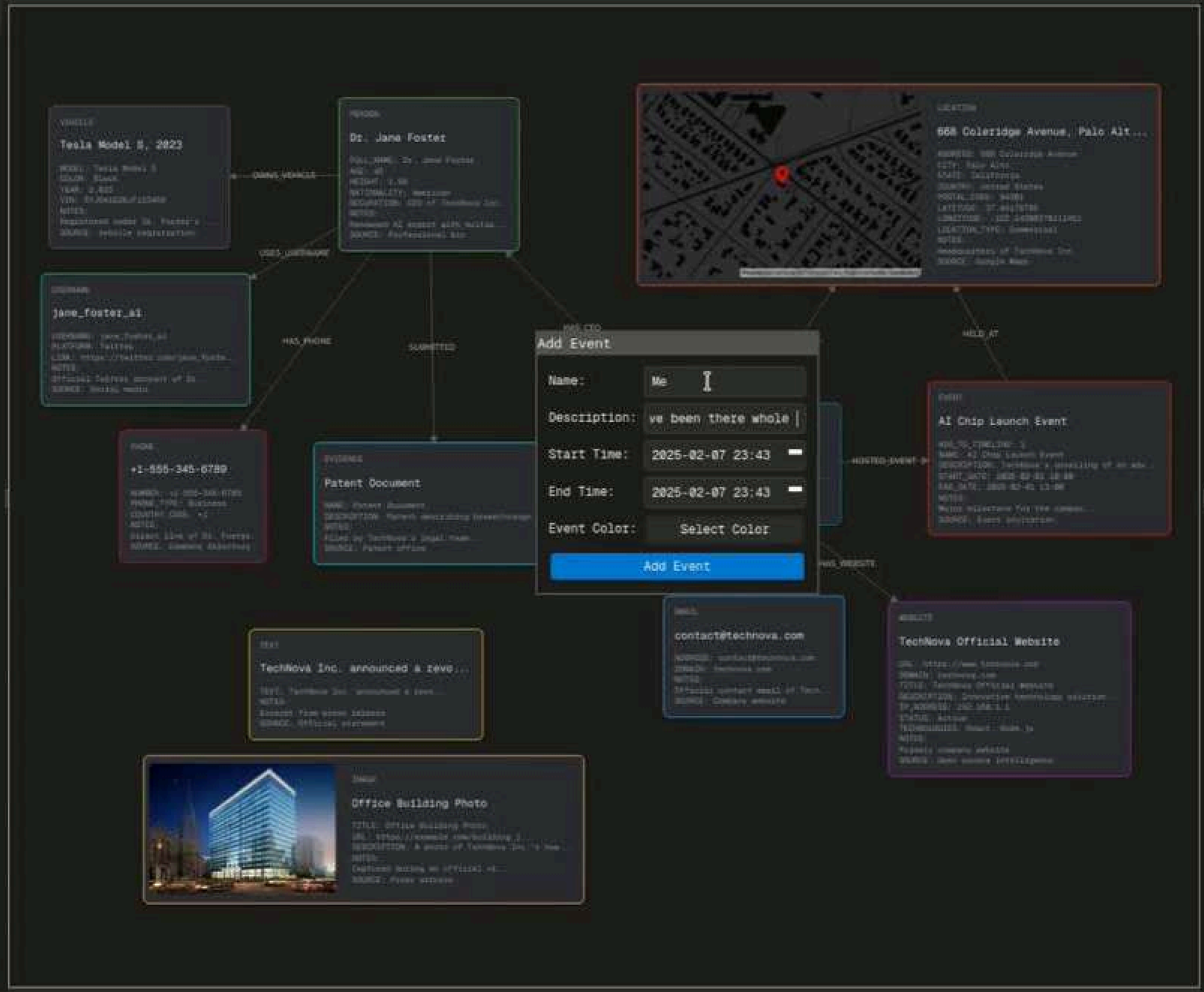
Entities

- Company
- Email
- Image
- Person
- Phone
- Text
- Username
- Vehicle
- Website
- Event
- Location
- Evidence

PANAI

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...



Timeline

01/02/25 10:00

AI Chip Launch Event

TechNova's unveiling of an advanced AI chip.

3h

01/02/25 13:00

Add Event

About

New | Save | Load | Windows | Search for a helper | Circular | Hierarchical | Radial | Force-Directed

ools

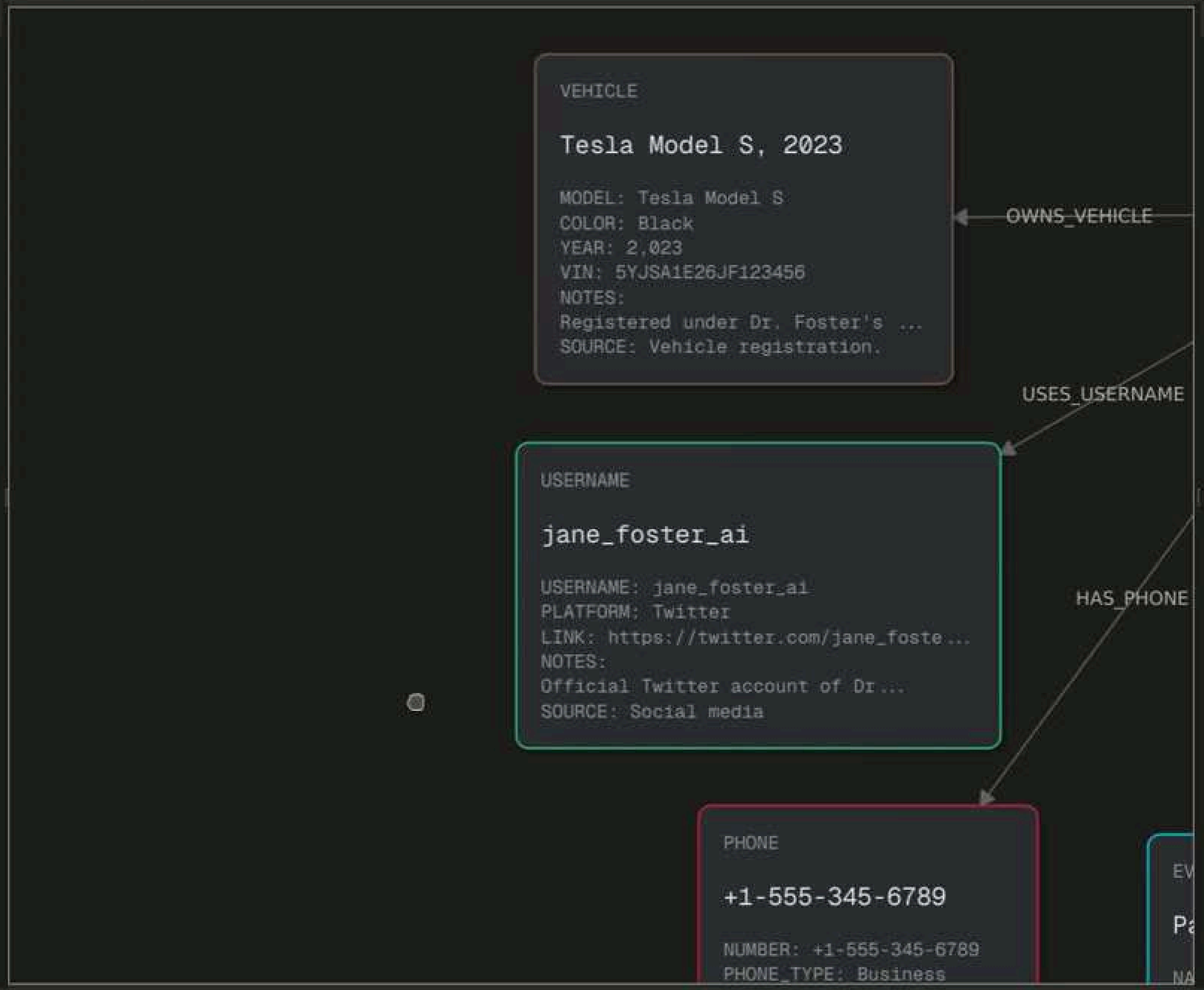
Entities

- Company
- Email
- Image
- Person
- Phone
- Text
- Username
- Vehicle
- Website
- Event
- Location
- Evidence

PANAI

You: Jane's username is actually jane4211

Describe what happened ...

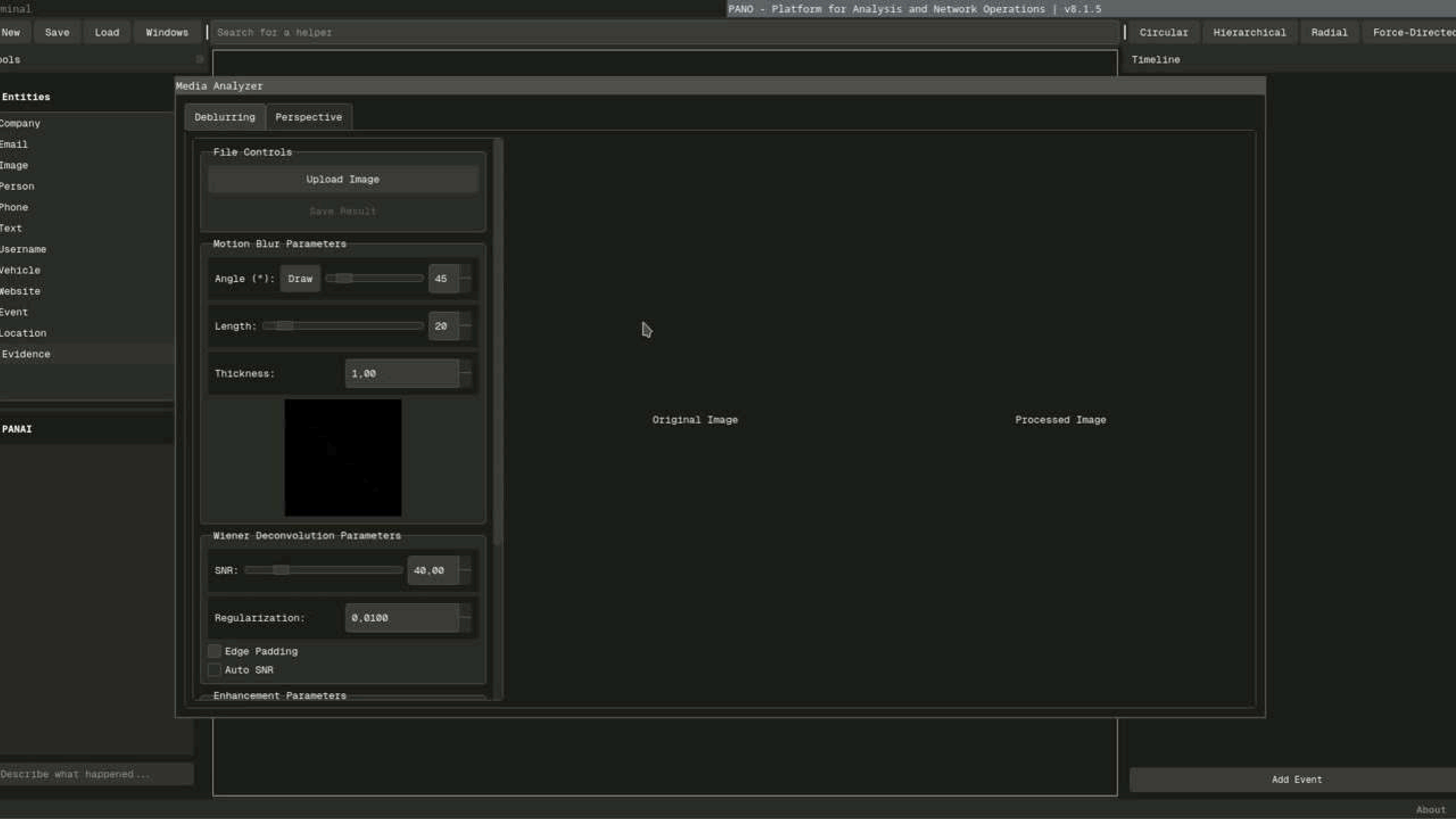


Timeline

01/02/25 10:00 — **AI Chip Launch Event**
TechNova's unveiling of an advanced AI chip.
3h

01/02/25 13:00

Add Event


minal
PANO - Platform for Analysis and Network Operations | v8.1.5
New
Save
Load
Windows
Search for a helper
Circular
Hierarchical
Radial
Force-Directed
ools
Timeline
Entities
Company
Email
Image
Person
Phone
Text
Username
Vehicle
Website
Event
Location
Evidence
PANAI
Describe what happened...
Add Event
About
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

New | Save | Load | Windows | Search for a helper

Circular | Hierarchical | Radial | Force-Directed

ools

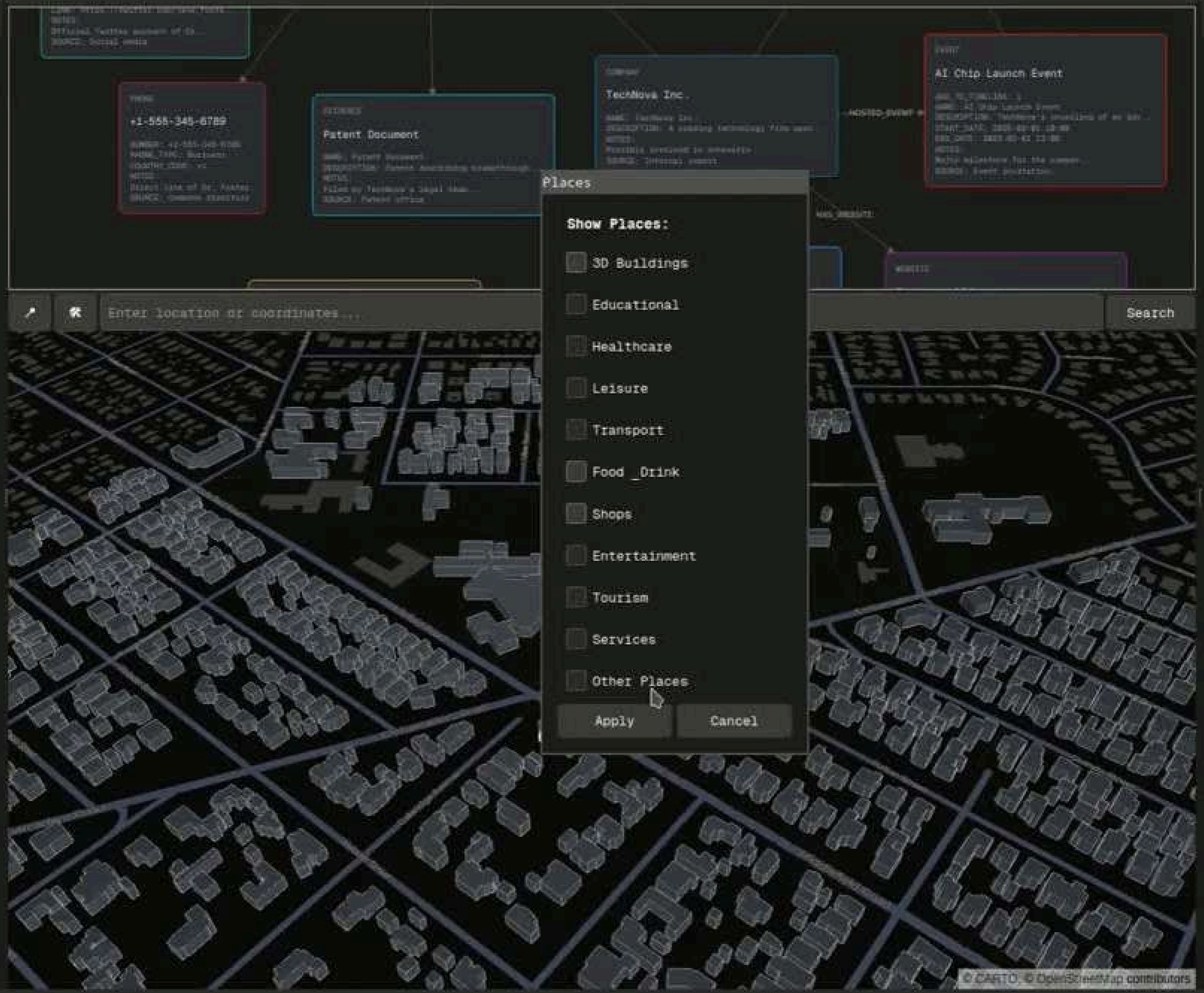
Entities

- Company
- Email
- Image
- Person
- Phone
- Text
- Username
- Vehicle
- Website
- Event
- Location
- Evidence

PANAI

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...



Timeline

01/02/25 09:00 — Don't know

01/02/25 10:00 — AI Chip Launch Event
TechNova's unveiling of an advanced AI chip.
3h

01/02/25 13:00

02/02/25 14:00
1d 5h

after 5d 9h 42mi

07/02/25 23:43 — Me
I have been there whole time

Add Event

About

minal

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

New | Save | Load | Windows | Search for a helper | Circular | Hierarchical | Radial | Force-Directed

ools

Timeline

Entities

Company
Email
Image
Person
Phone
Text
Username
Vehicle
Website
Event
Location
Evidence

PANAI

Describe what happened...

Add Event

Text Translator

Source Text:

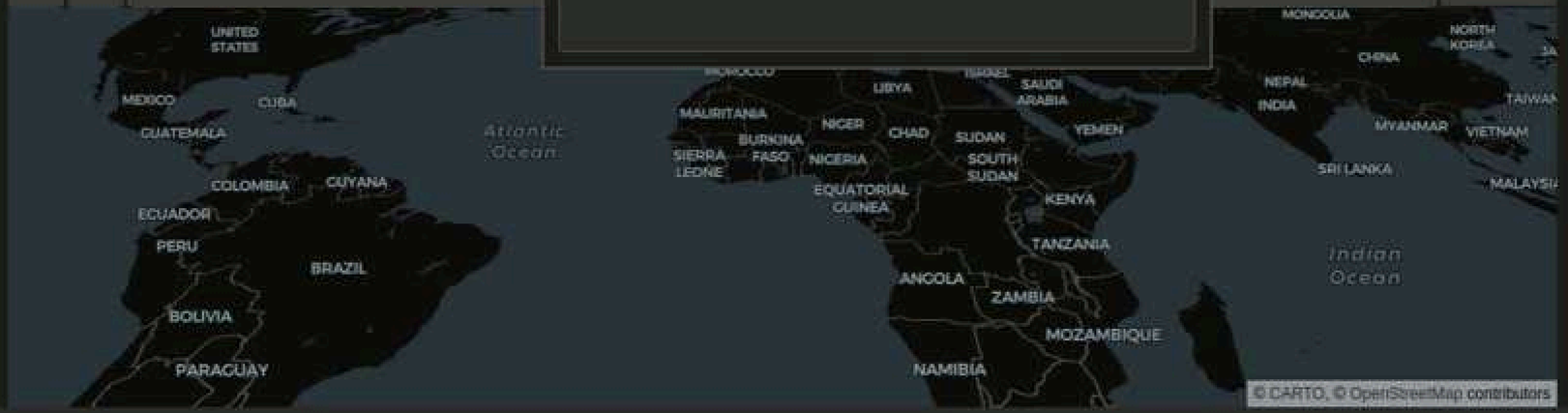
s

Detected Language: None

Target Language: english

Translation:

Enter location or coordinates... | Search



About

minal

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

New | Save | Load | Windows | Search for a helper | Circular | Hierarchical | Radial | Force-Directed

ools

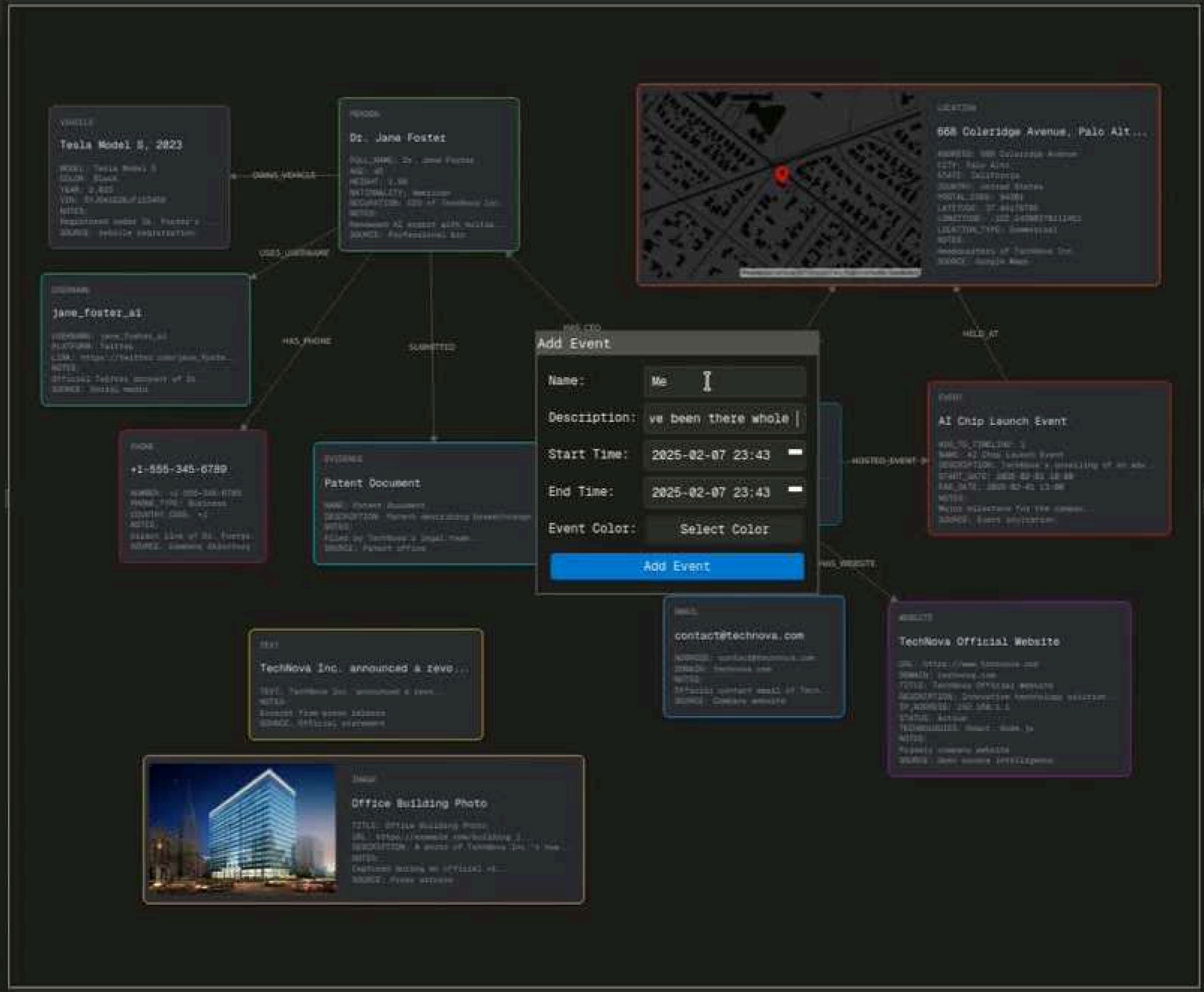
Entities

- Company
- Email
- Image
- Person
- Phone
- Text
- Username
- Vehicle
- Website
- Event
- Location
- Evidence

PANAI

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...



Timeline

01/02/25 10:00

AI Chip Launch Event

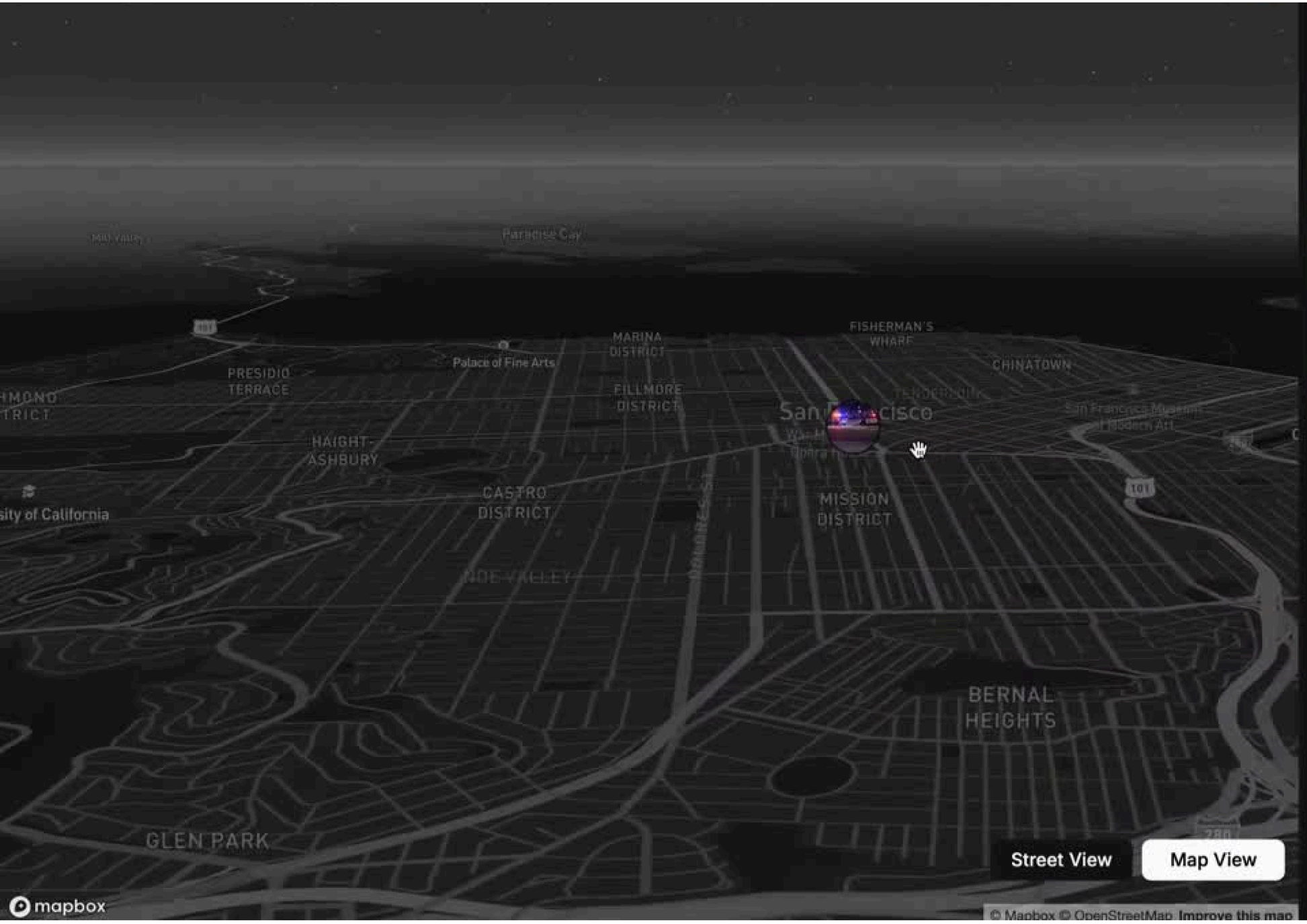
TechNova's unveiling of an advanced AI chip.

3h

01/02/25 13:00

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

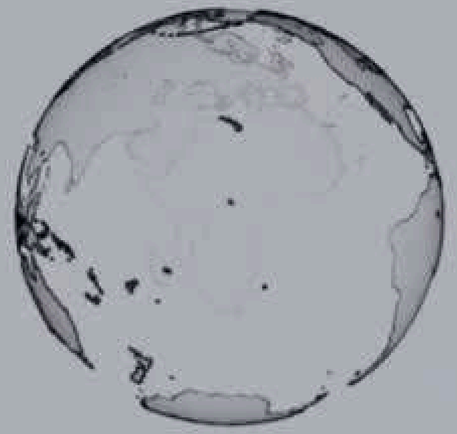
Camera Type:
samsung

Camera Model:
Galaxy S24 Ultra

Export PDF

Share Geospy

How'd we do?

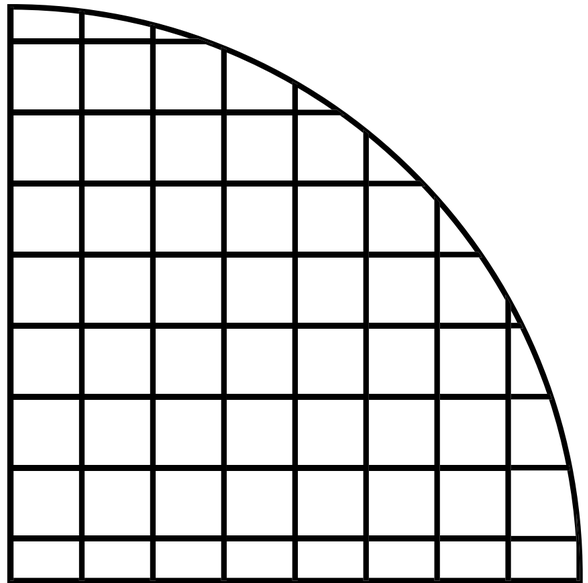


Covert Cabal

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, eligib
leforsignupbonus",
    "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 kenings
ton 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://shop
ify/Customer/7661420281954"
  },
  {
    "id": 7661420150882,
    "email": "niveditachoudhary2000@gma
il.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, eligib
leforsignupbonus",
    "last_order_name": null,
    "currency": "INR",
    "phone": "+919654776817",
    "addresses": [],
    "tax_exemptions":~/do~/downloa~/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.

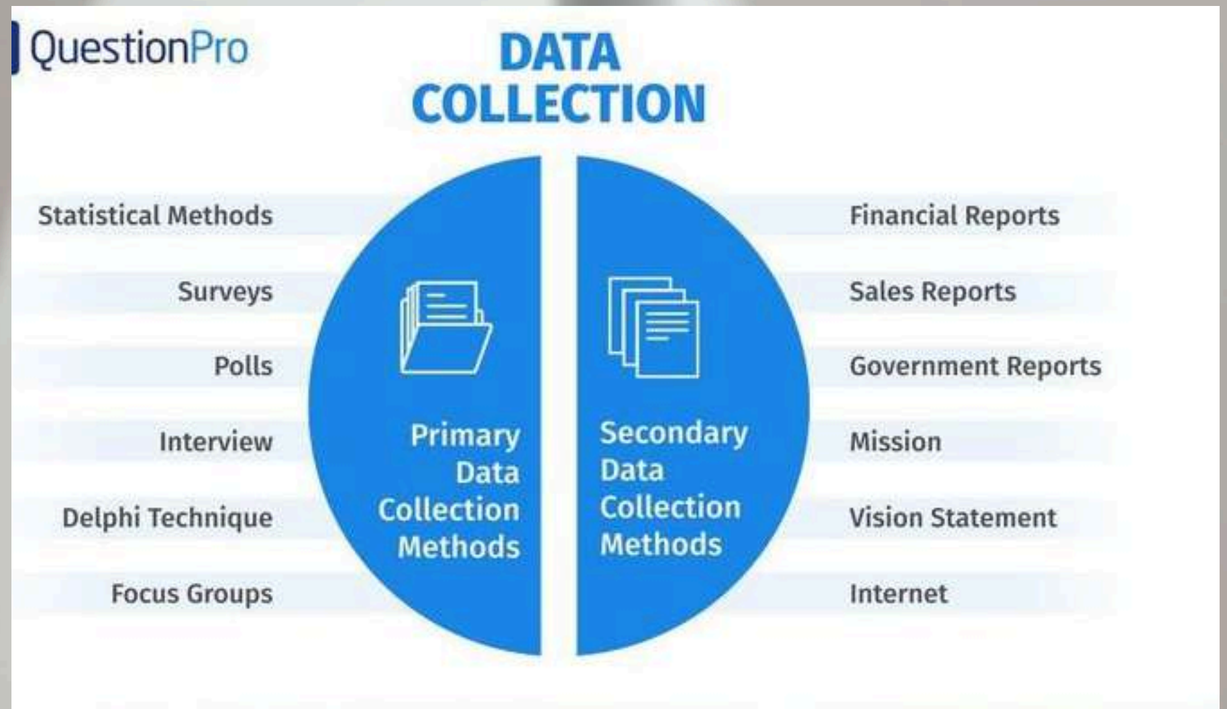
Israel Says It Killed Hezbollah Commander in Airstrike Near Beirut

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?

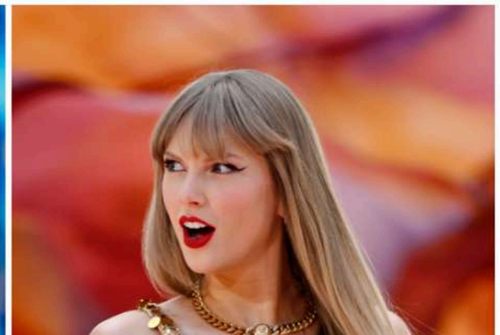
Why OSINT is Crucial?

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.

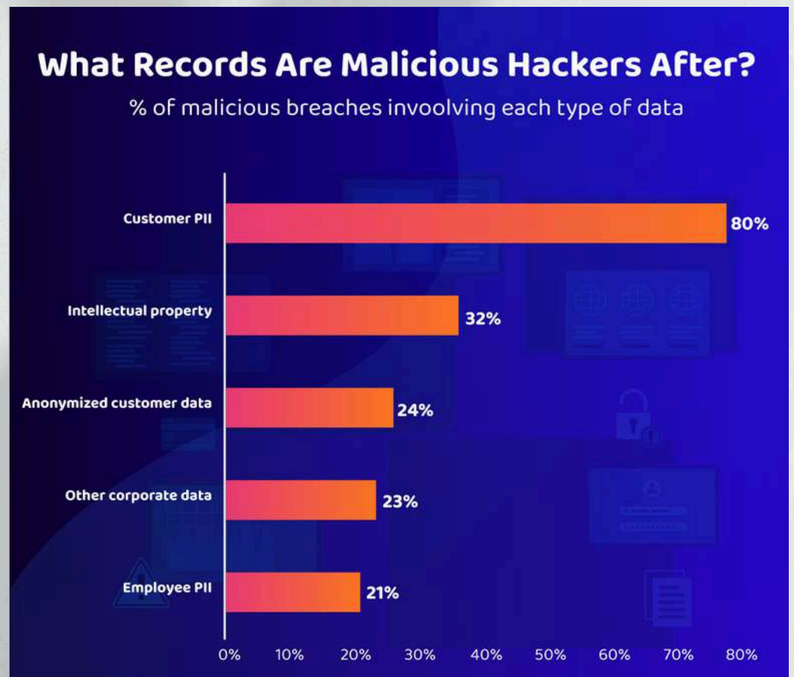
By Amanda Yeo on July 5, 2024



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.

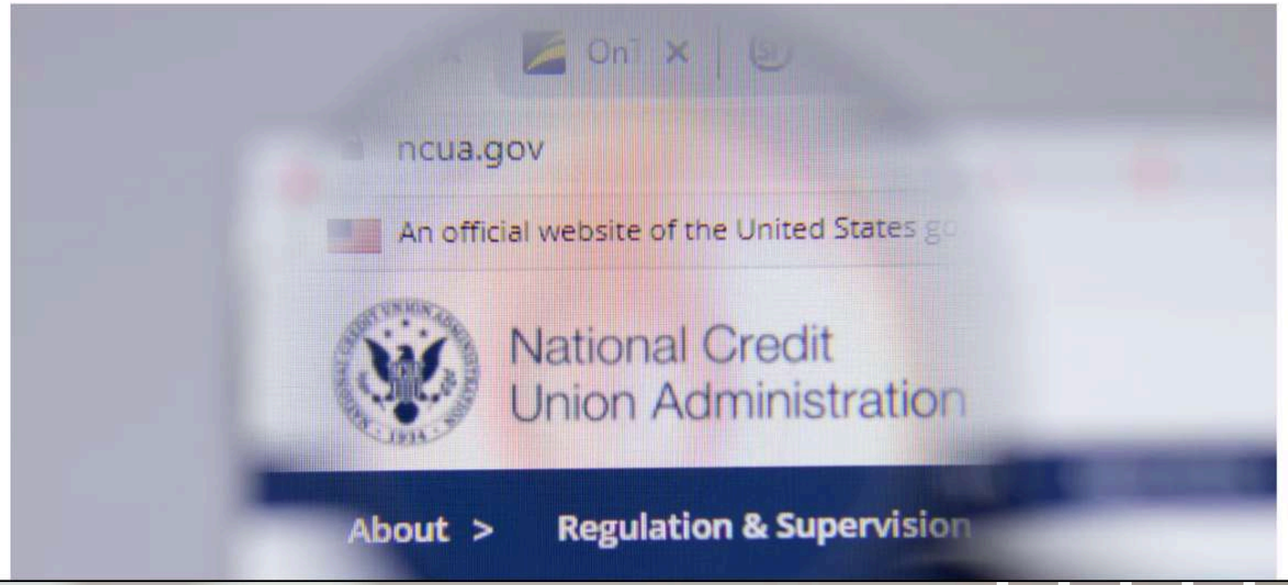
Listen to Story

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



MORE FROM CNN

NEWS & BUZZ

OSINT Techniques

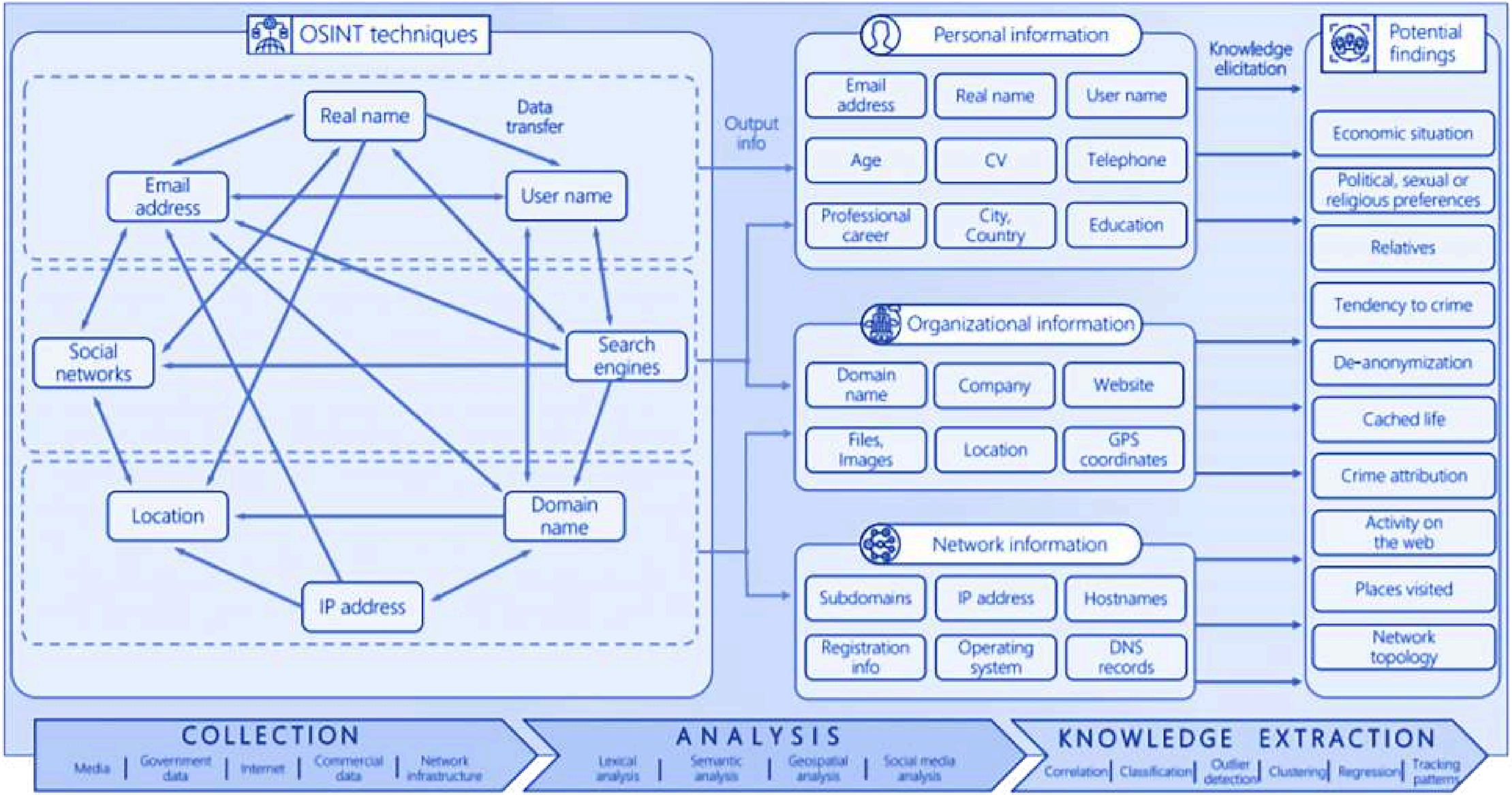
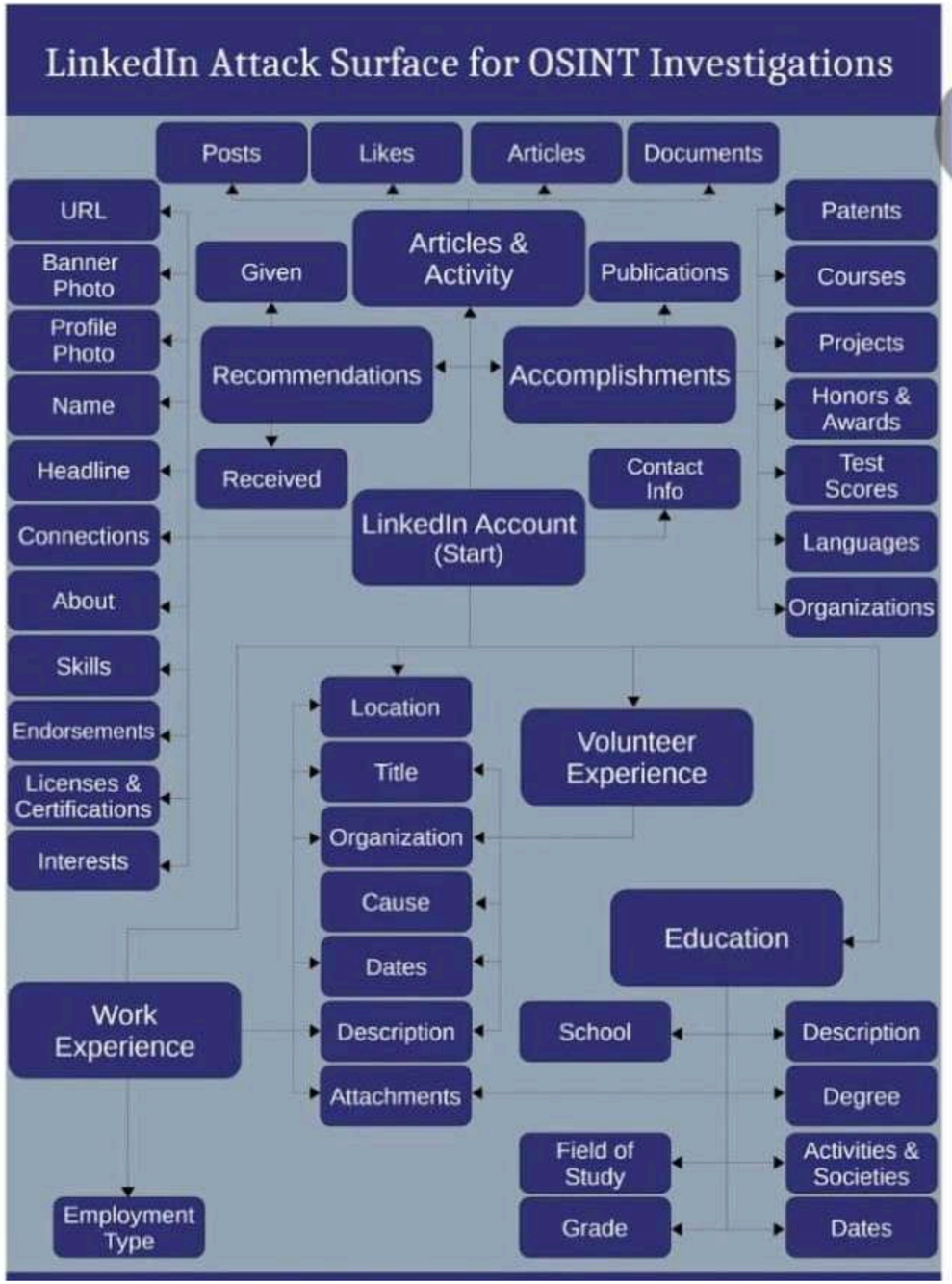


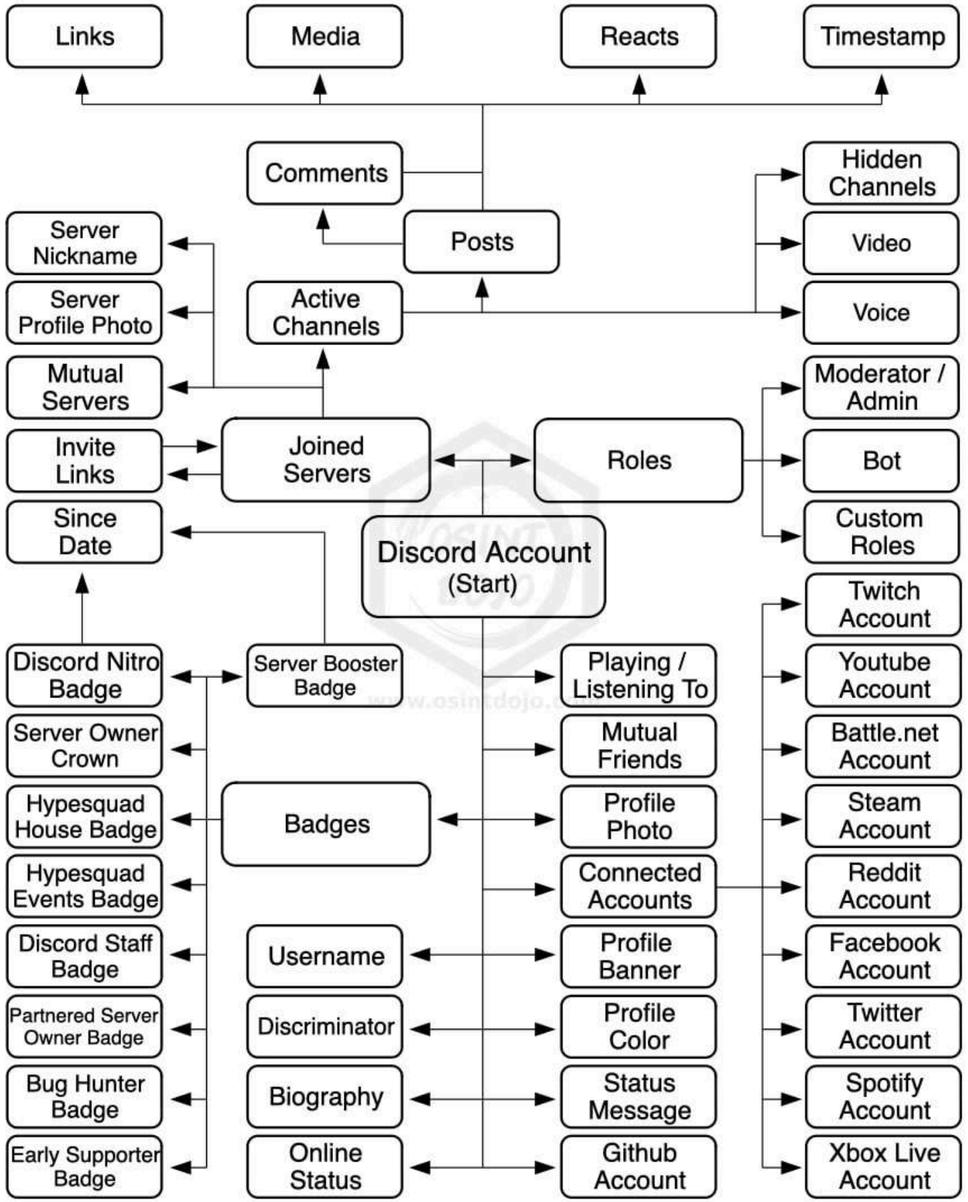
FIGURE 2. Principal OSINT workflows and derived intelligence.



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.

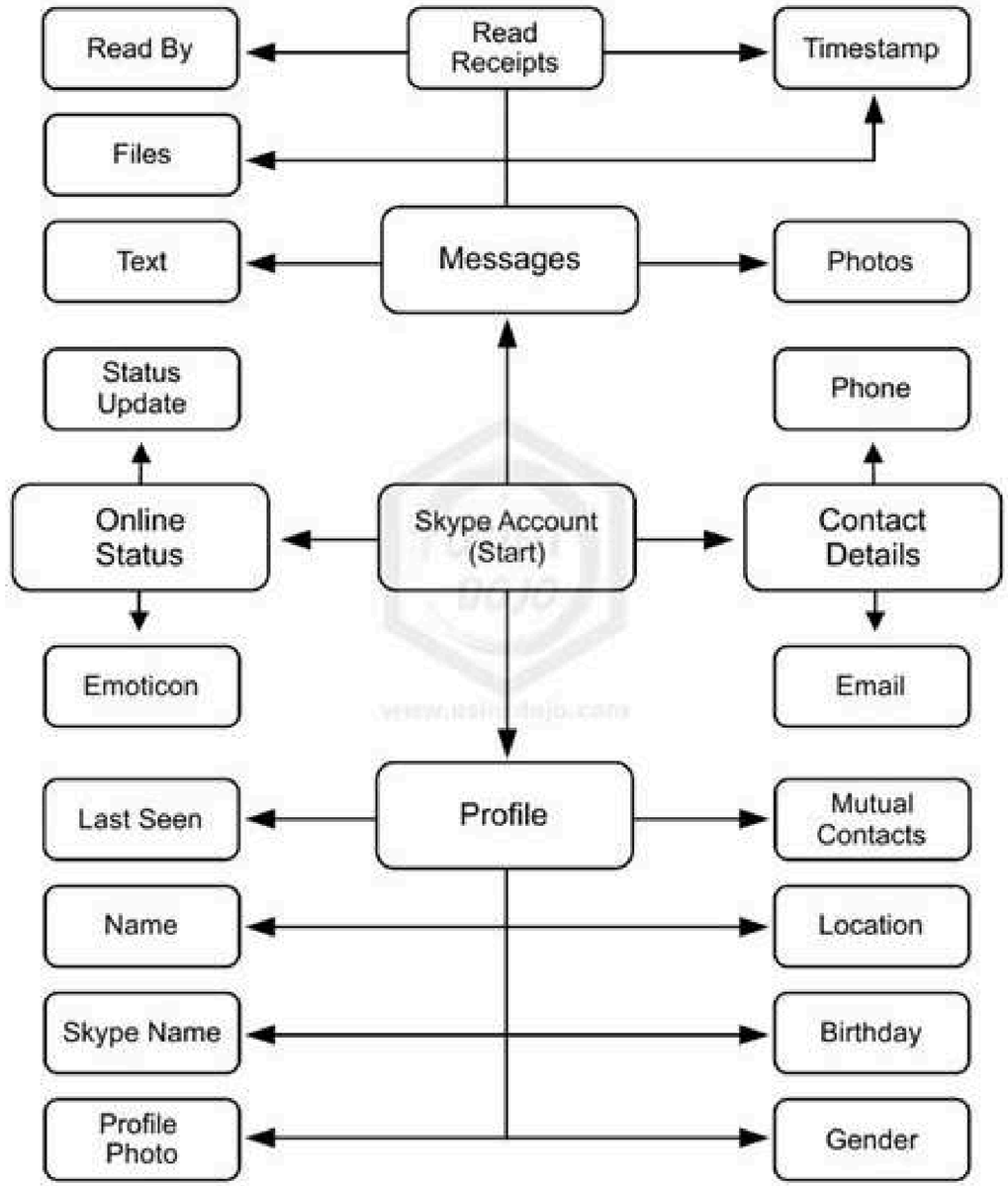


Discord OSINT

- 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.

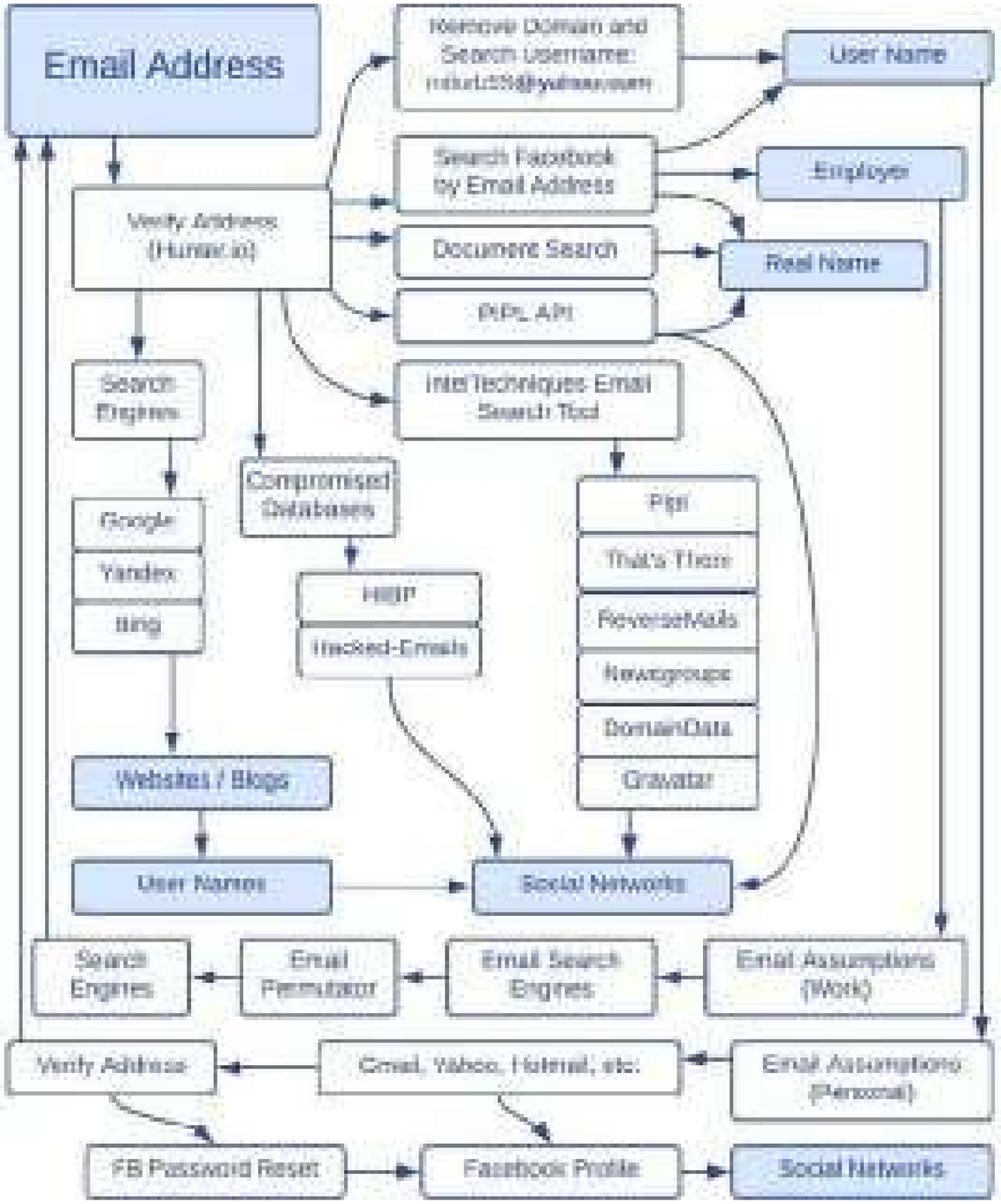


Skype OSINT

- 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.

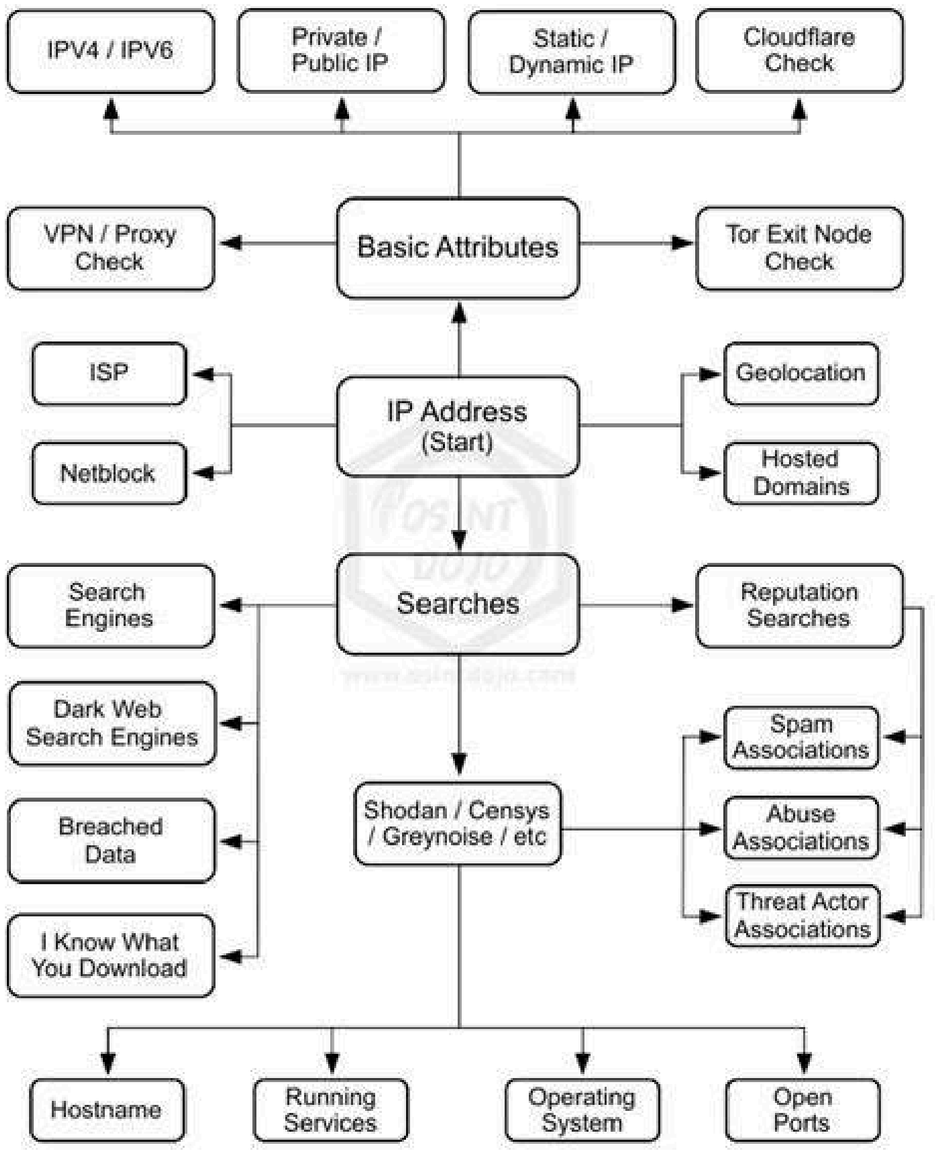


Email Osint

- 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.



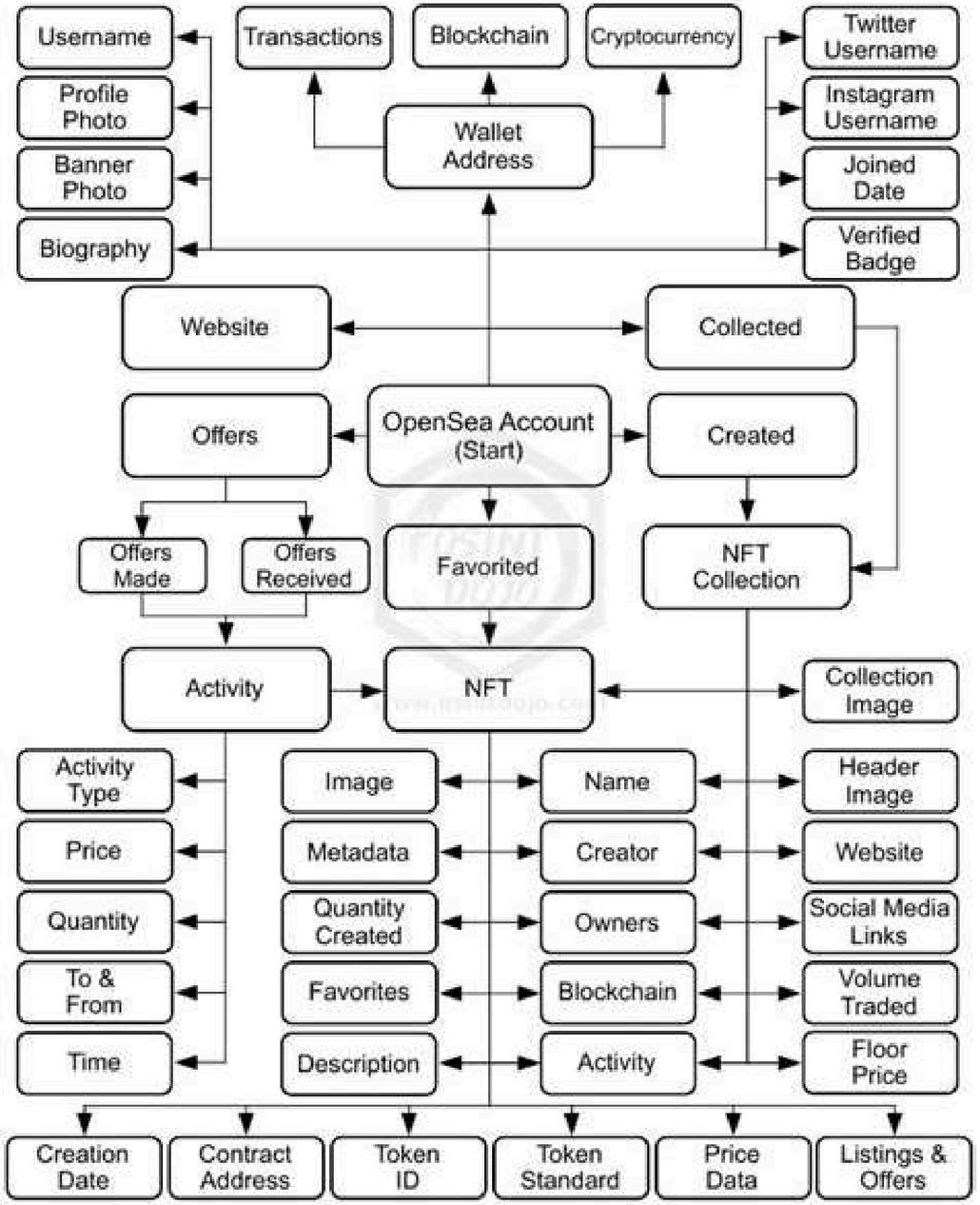
IP Address

- 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.

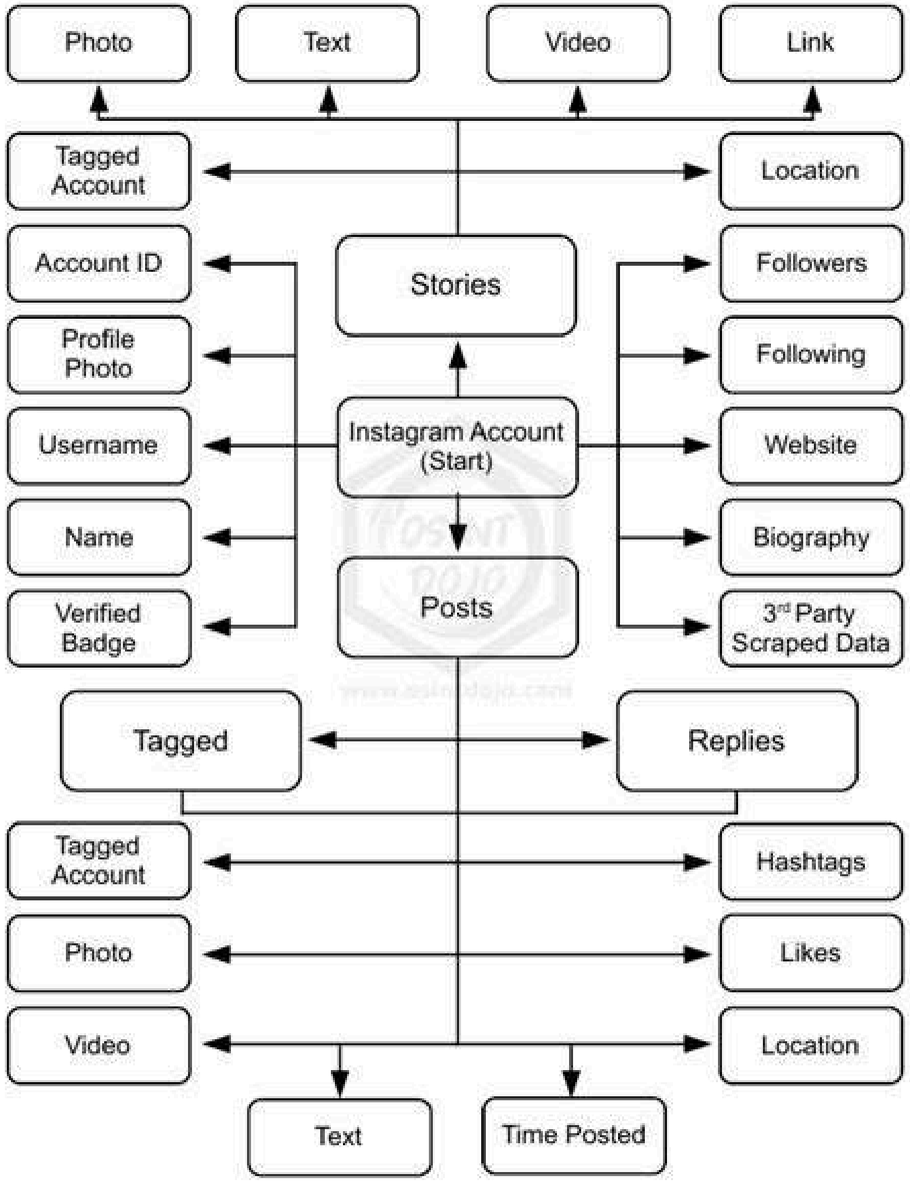
OpenSea Osint



- 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.

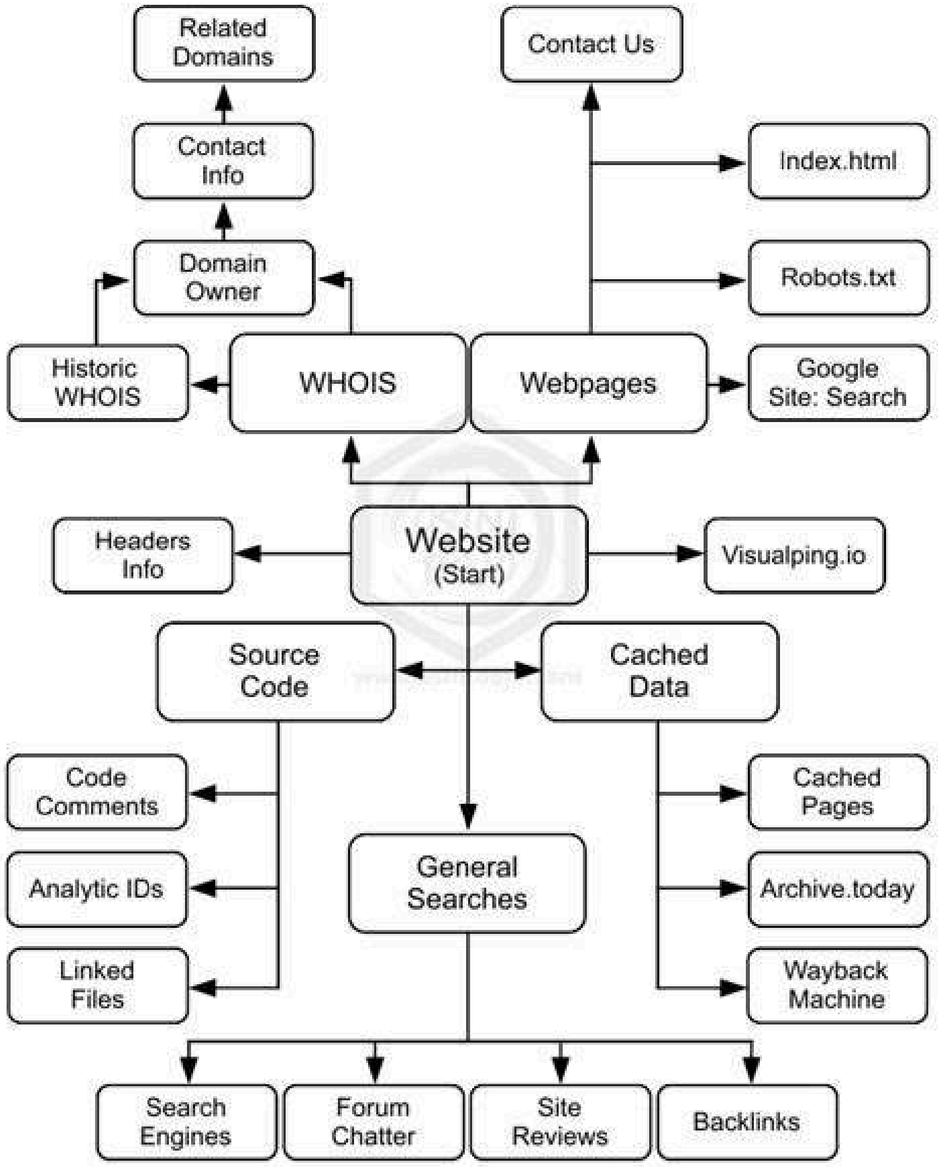


Instagram Osint

- 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.



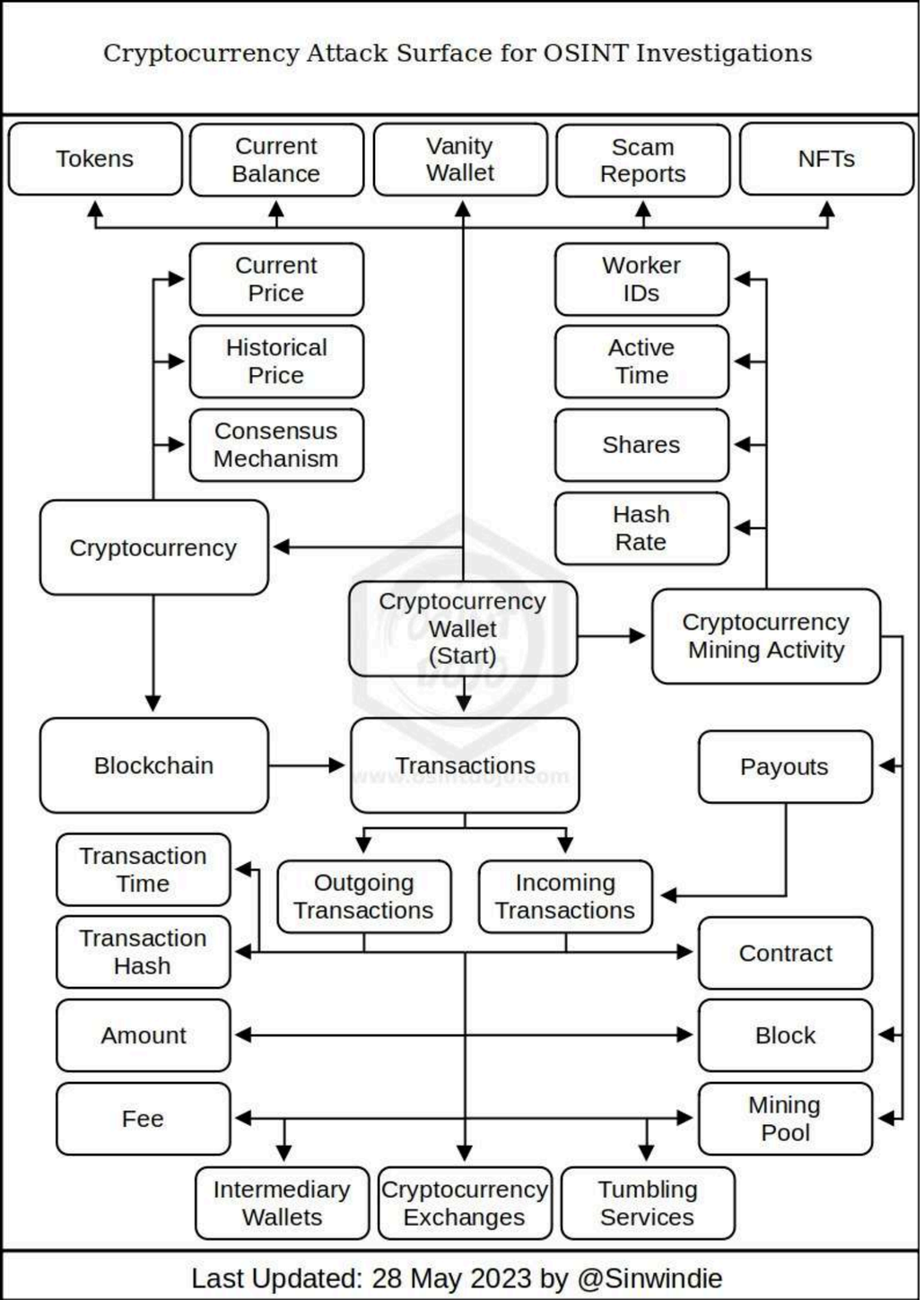
Website Osint

- 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.



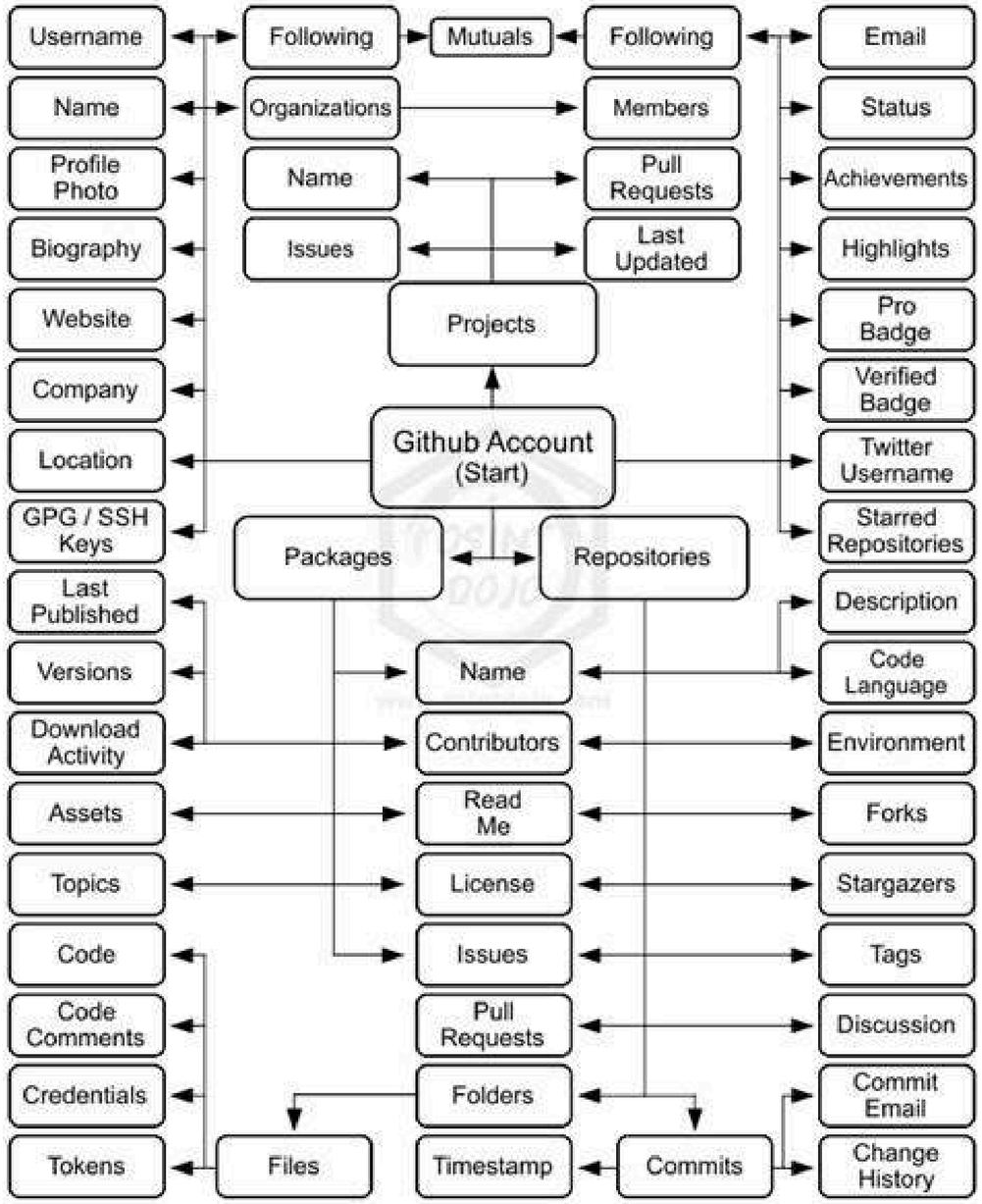
Cryptocurrency Osint

- 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

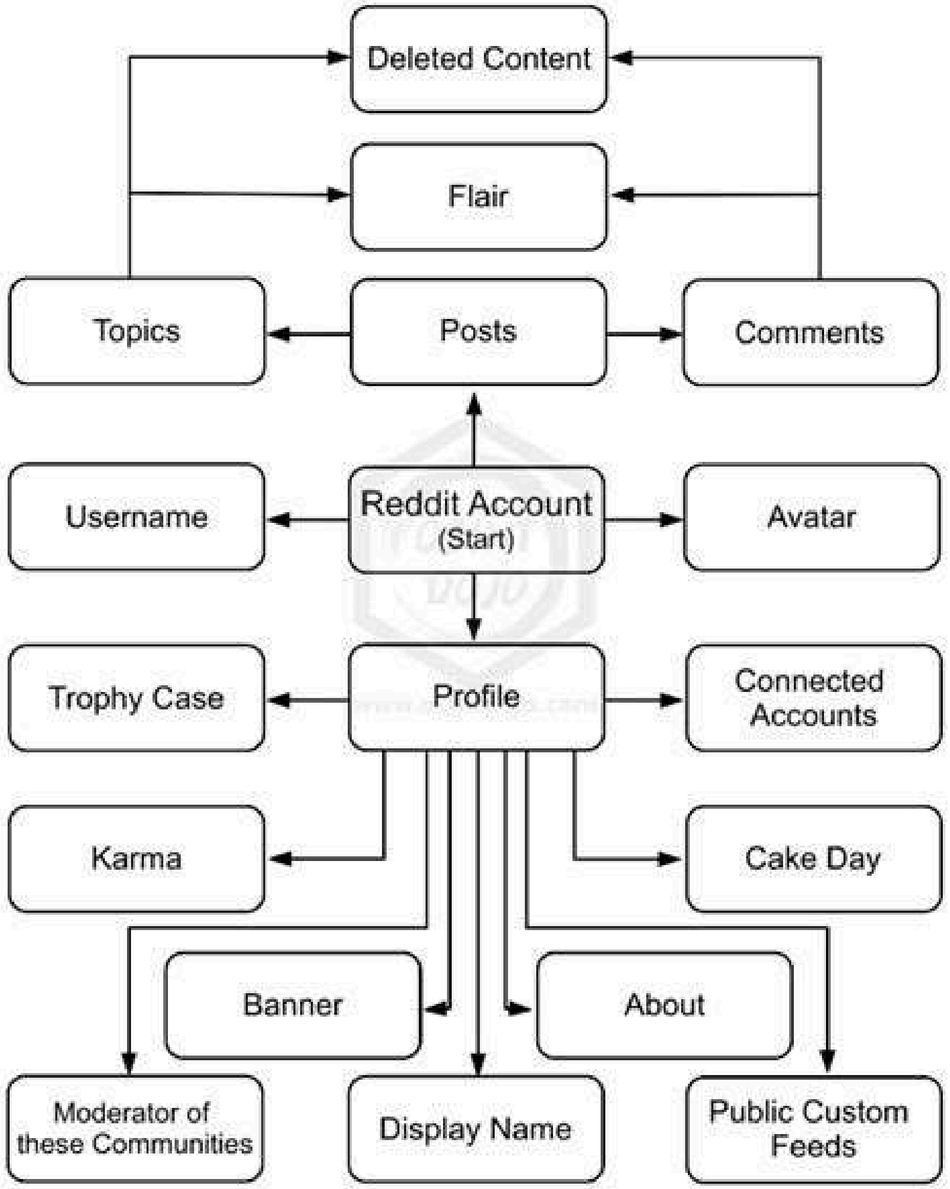
- Tools:
  - Blockchain Explorer – Tracks Bitcoin transactions.
  - CipherTrace – Identifies illicit cryptocurrency flows.
- Exploits:
  - Wallet reuse allows deanonymization.
- News:
  - 2023: Chainalysis uncovered $20B in illicit crypto transactions.

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.

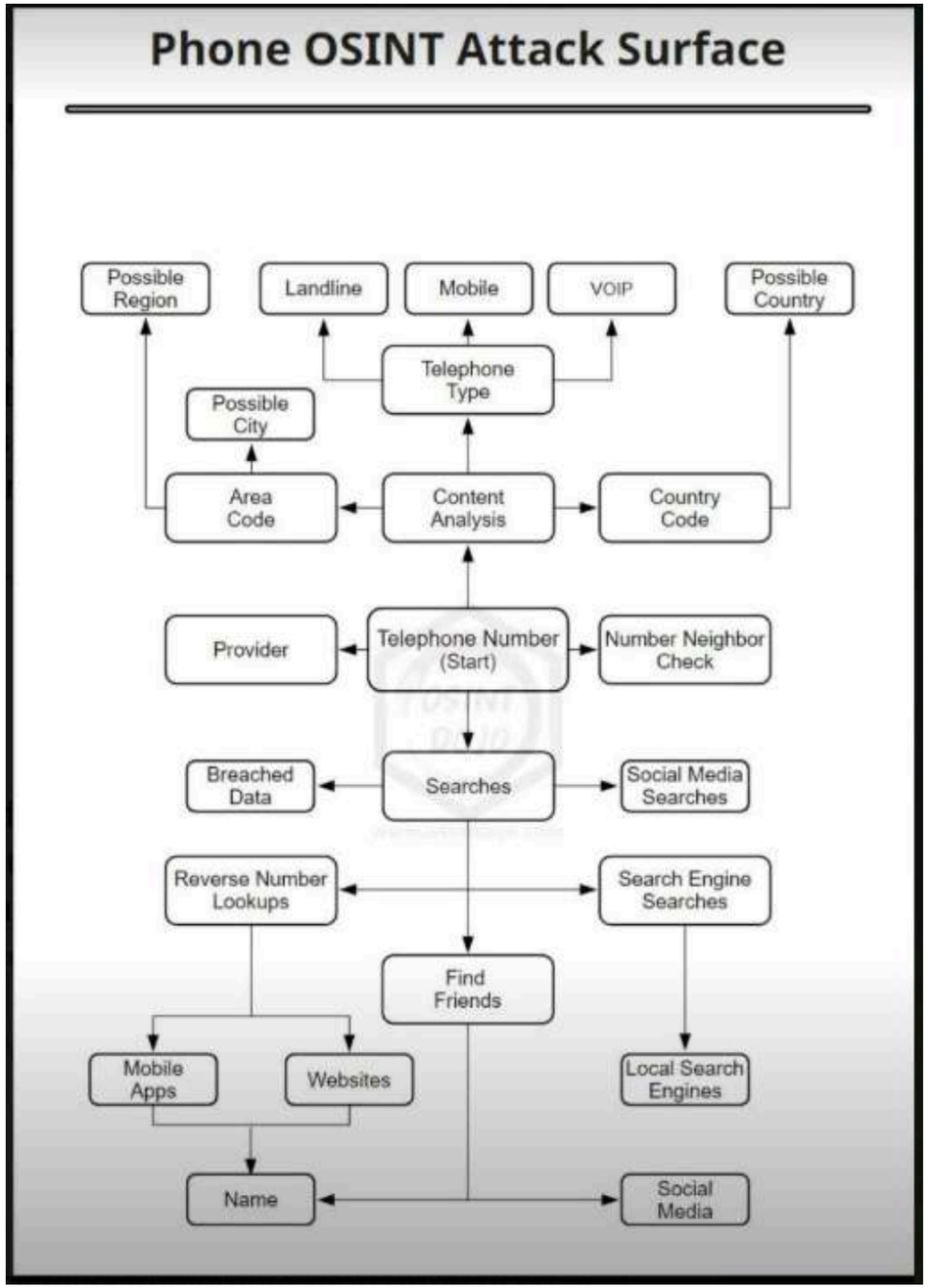


Reddit Account

- 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.

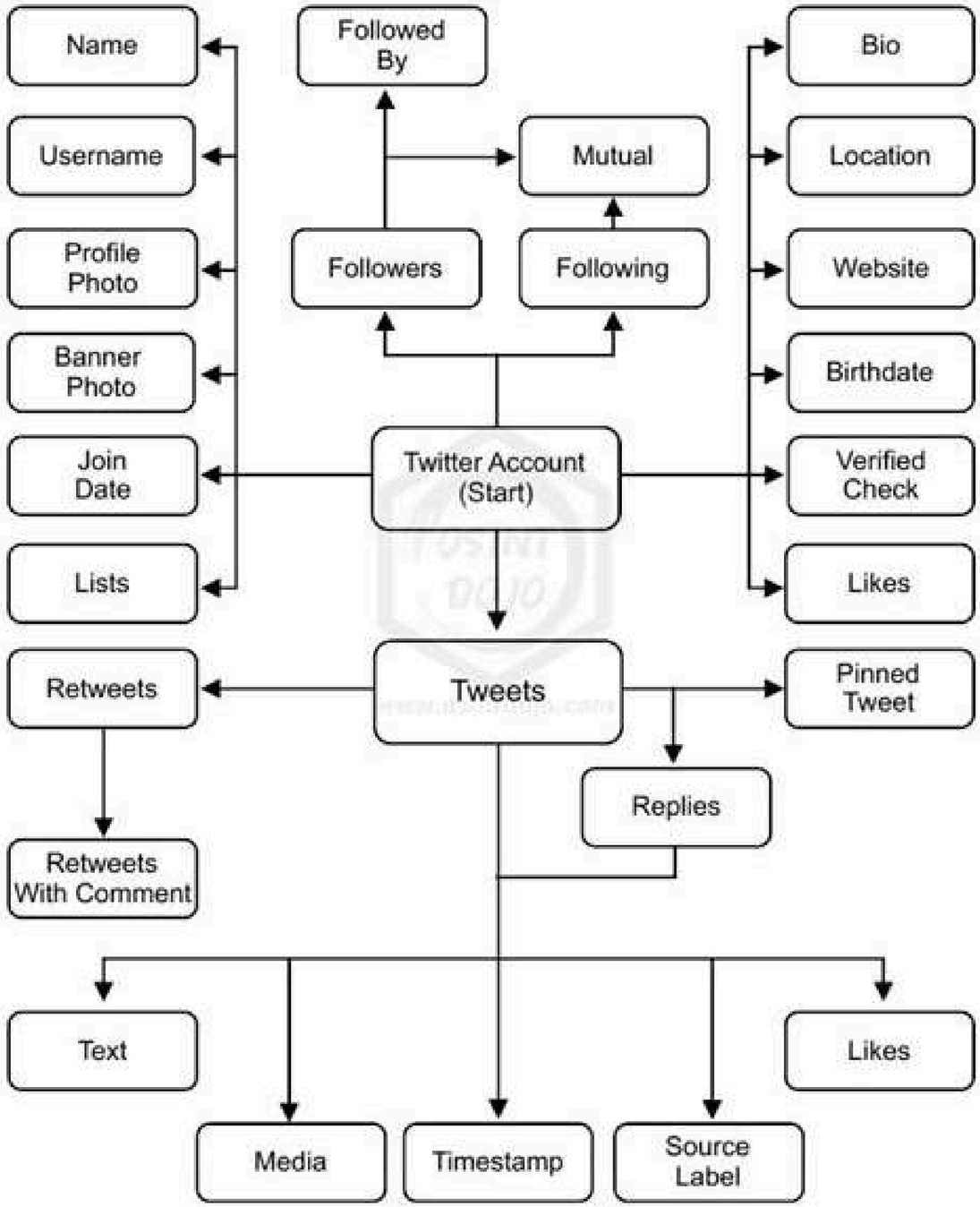


Phone Osint

- 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.

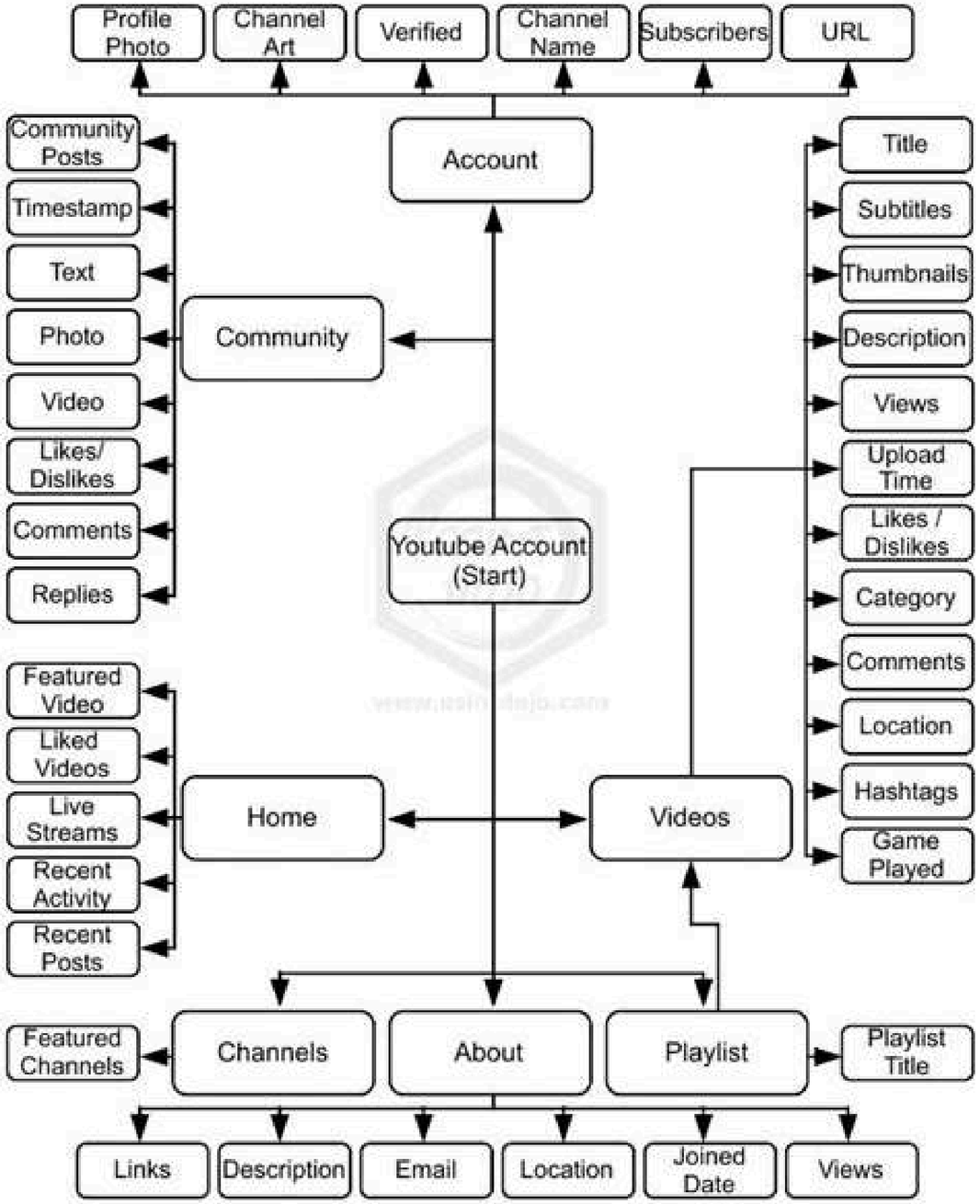


Twitter Osint

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

5. Twitter OSINT

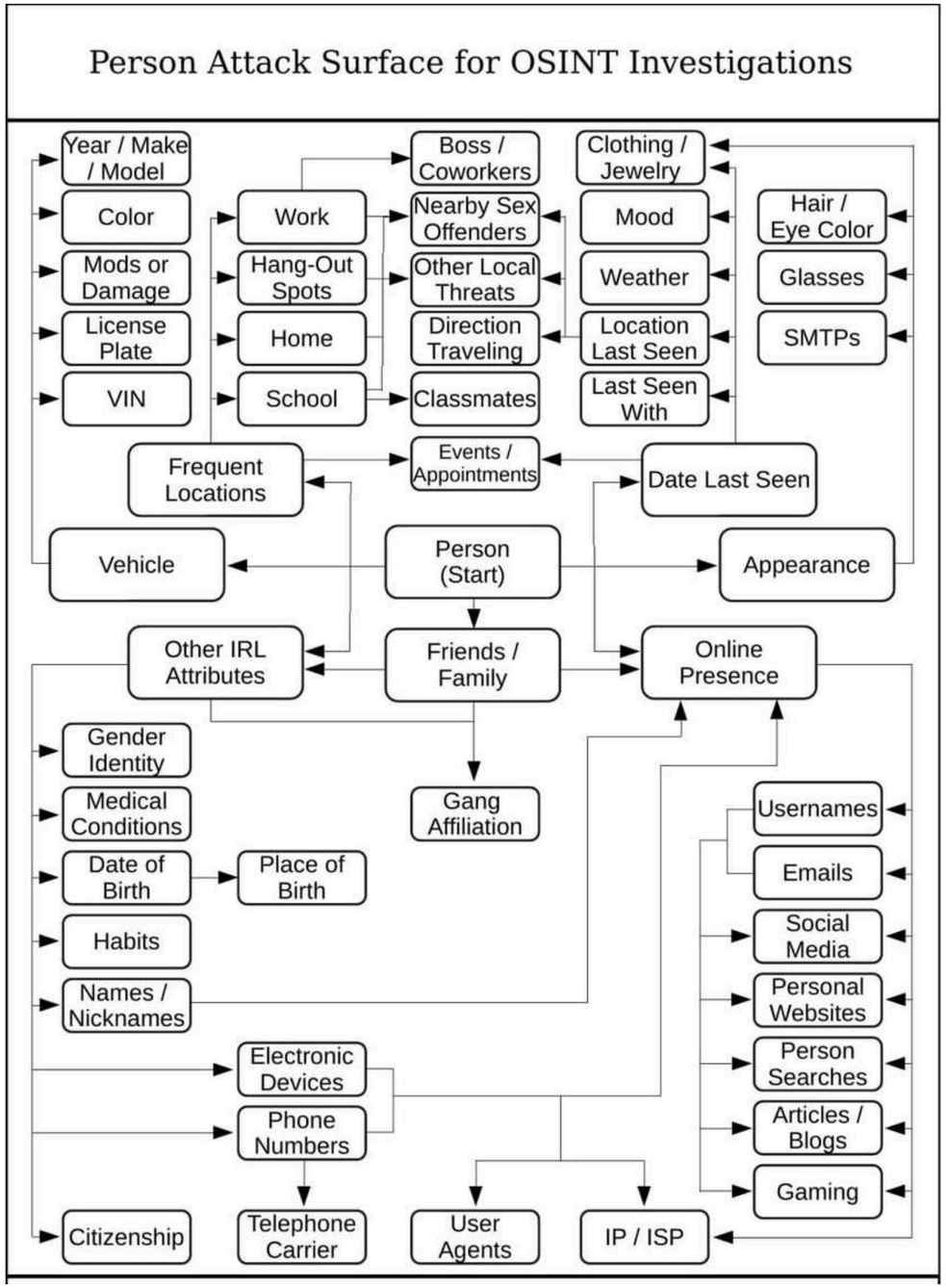
- Tools:
  - Twint – Scrapes Twitter data without API limits.
  - TweetBeaver – OSINT automation for Twitter.
- Exploits:
  - Deleted tweets still accessible via third-party archives.
- News:
  - 2023: Twitter API leaks exposed 200M user emails.



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.

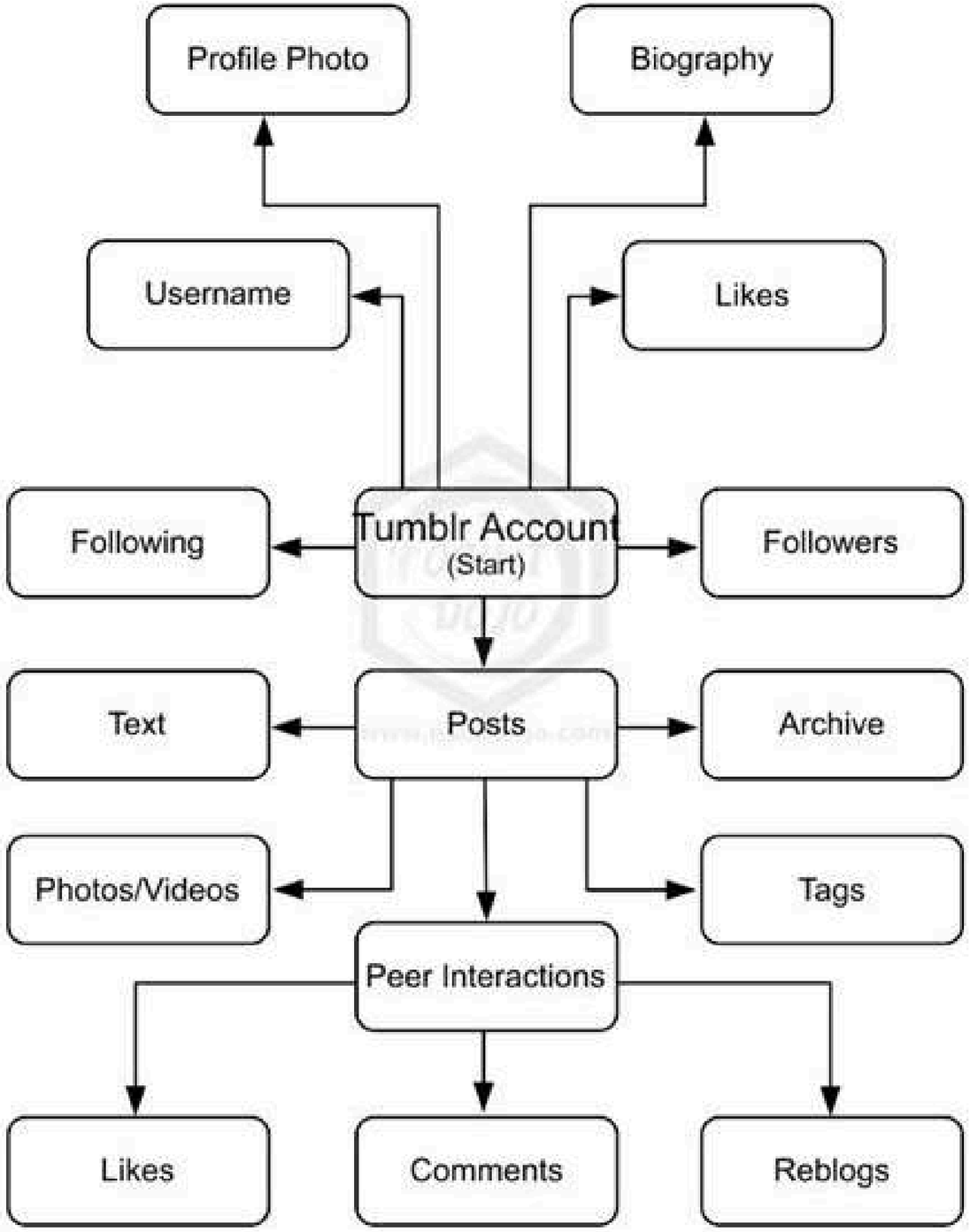
YouTube OSINT Tools – YouTube Metadata Tool, InVID, YouTube Data API for tracking video metadata, timestamps, and geolocation.



Person Osint

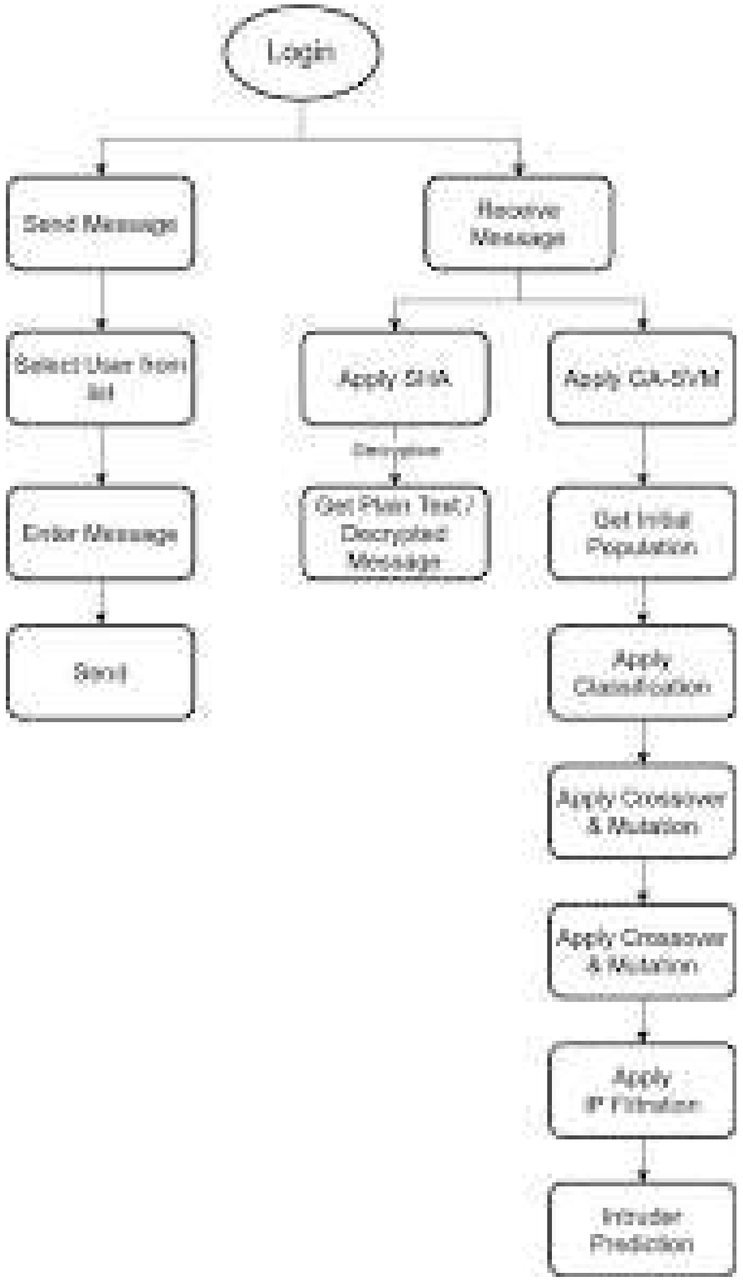
- Explores Person OSINT, which involves gathering data on individuals.
- Covers search engine techniques, social media footprint tracking, and database searches.
- Highlights risks of personal data leaks through public records.
- Suggests privacy best practices for securing personal information.

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



Tumblr Osint

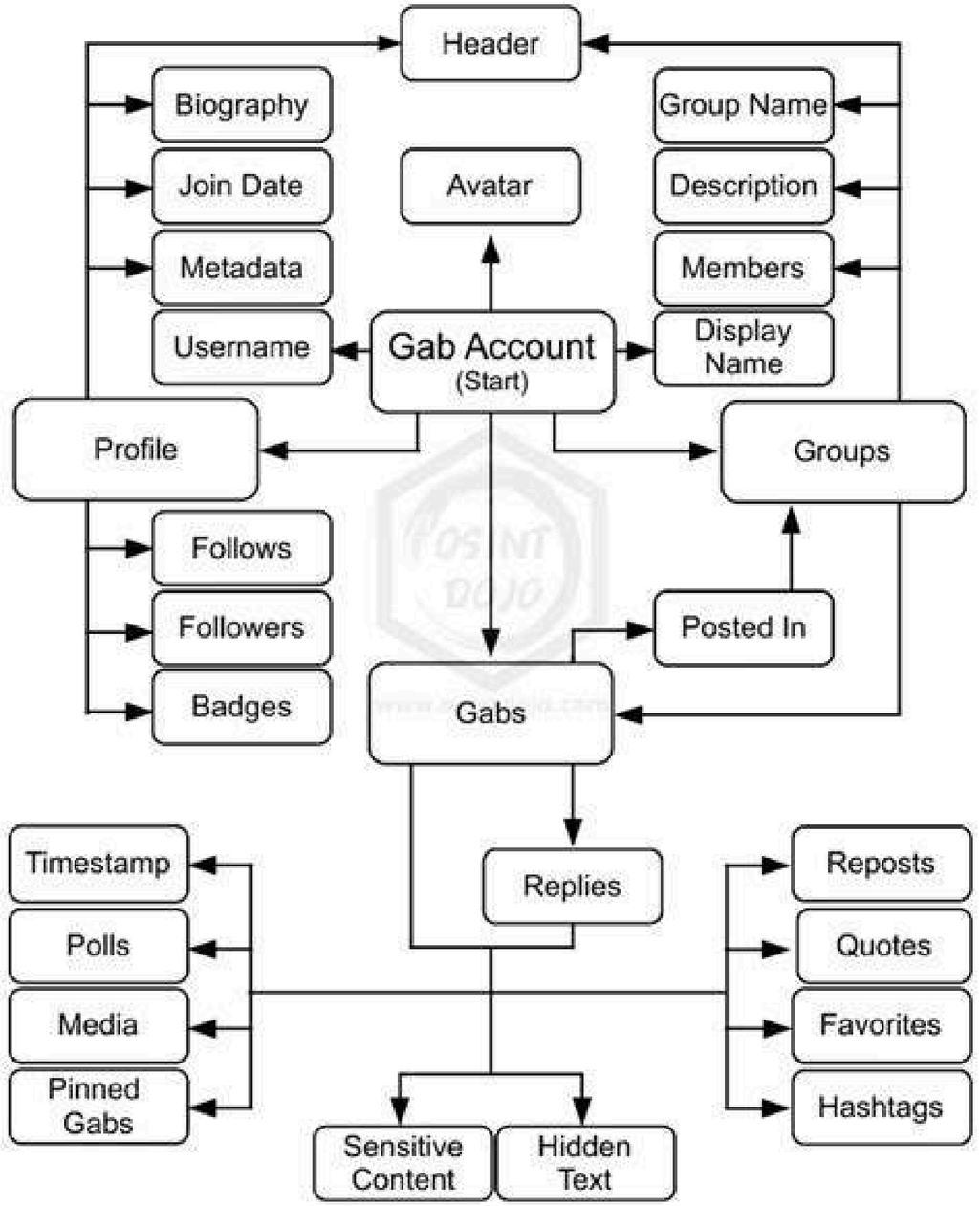
- Covers Tumblr OSINT, emphasizing blog activity monitoring.
- Discusses how Tumblr posts and comments can be used for intelligence gathering.
- Highlights risks of exposing personal data through old Tumblr posts.
- Recommends securing Tumblr accounts to minimize OSINT exposure.



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.

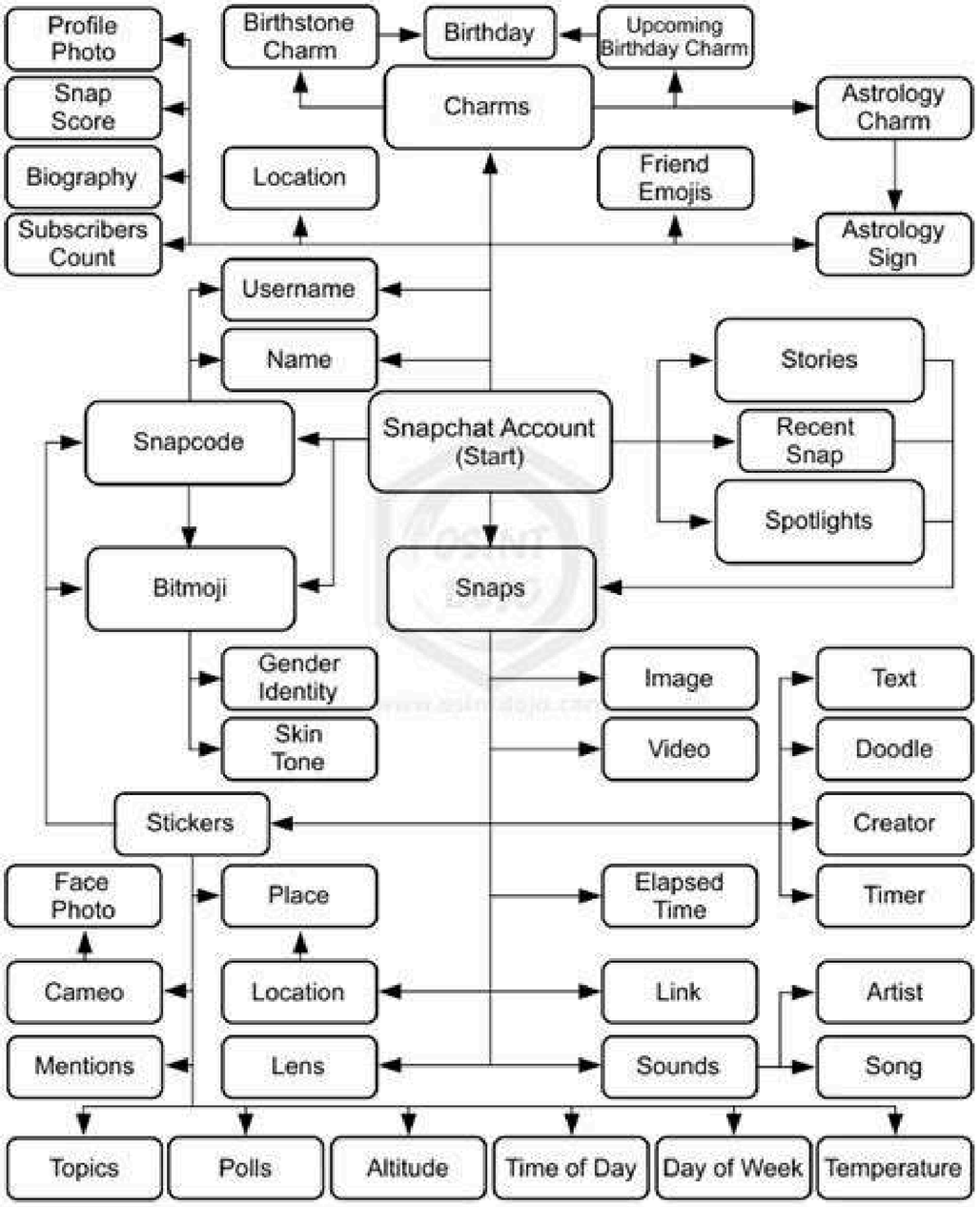
Login OSINT Tools – Have I Been Pwned, Dehashed, and Snusbase for tracking leaked credentials



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.

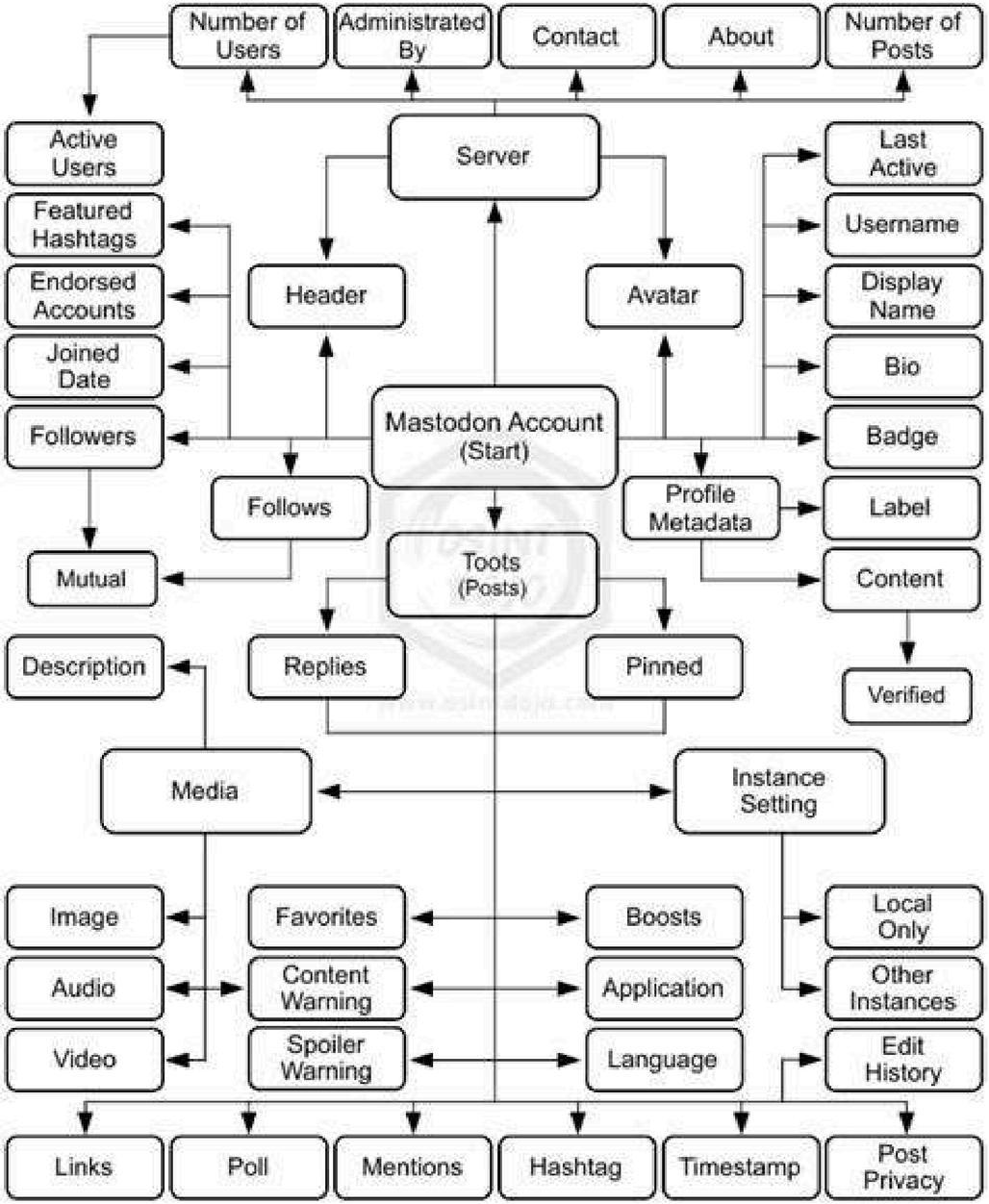
Gab OSINT Tools – Gab API monitoring, OSINT Framework for extremist tracking, and social network analysis.



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.

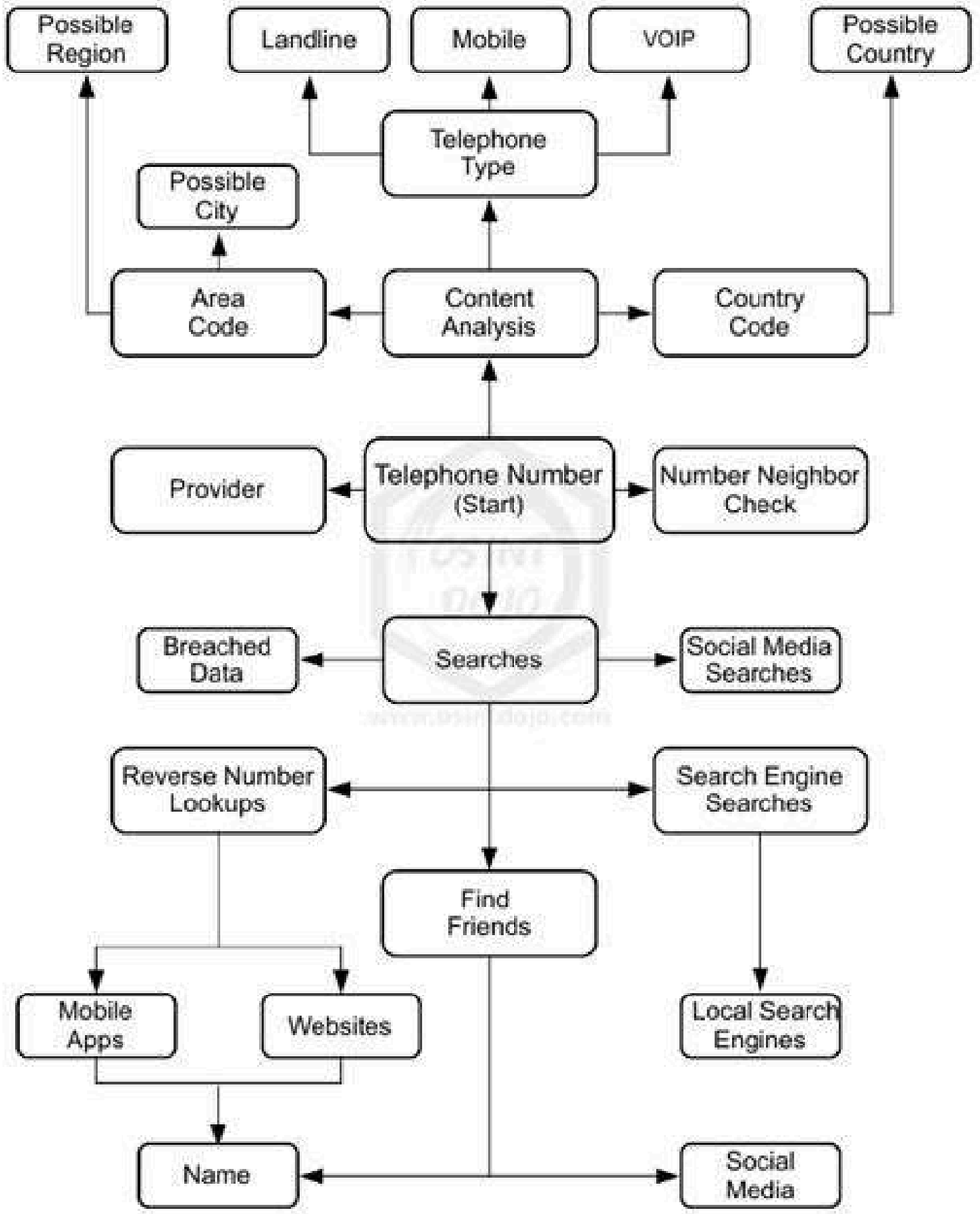
Snapchat OSINT Tools – Snap Map, ExifTool for metadata extraction, and forensic analysis tools.



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.

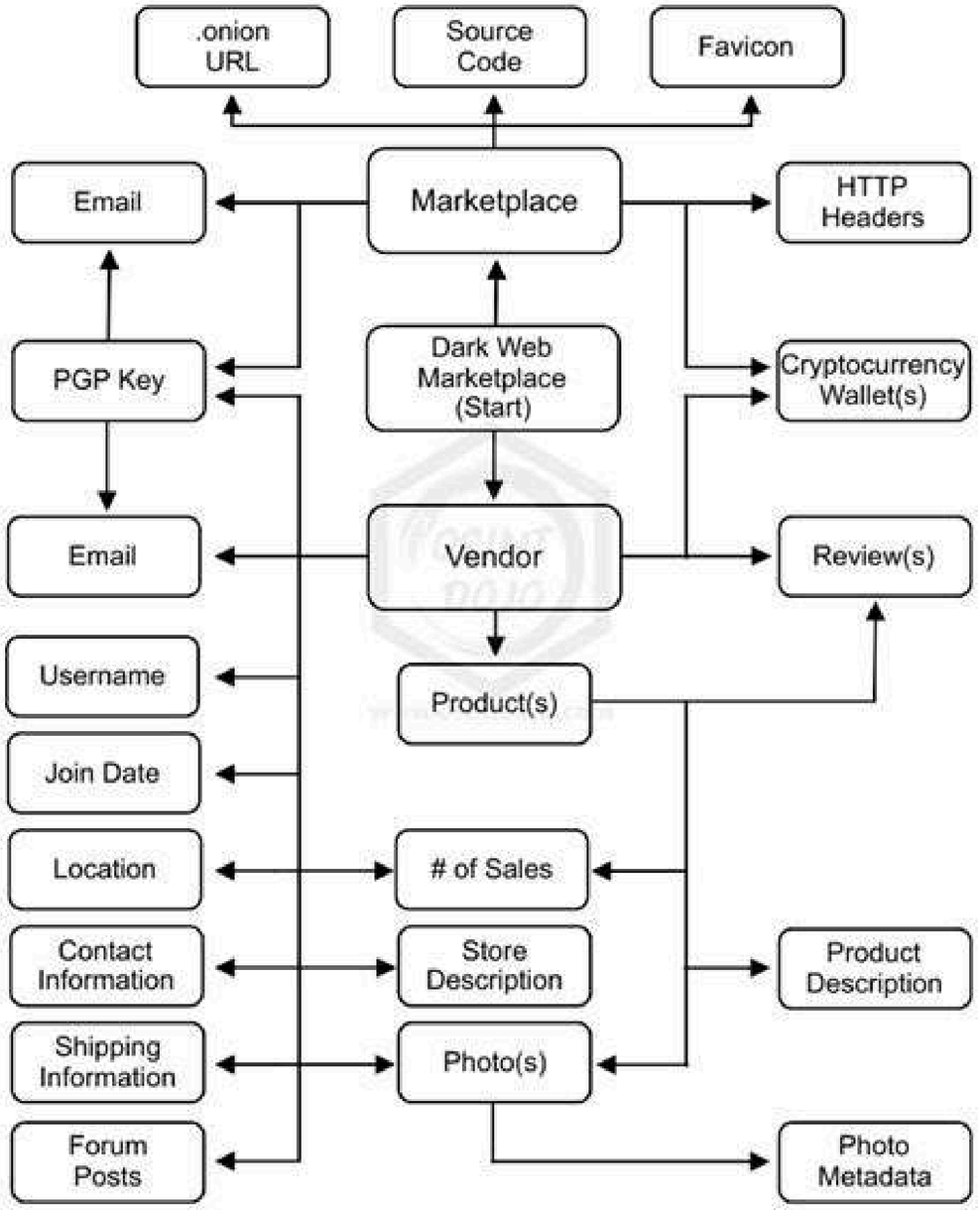
Mastodon OSINT Tools– Fediverse.tools, TheHarvester for federated social media tracking.



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.

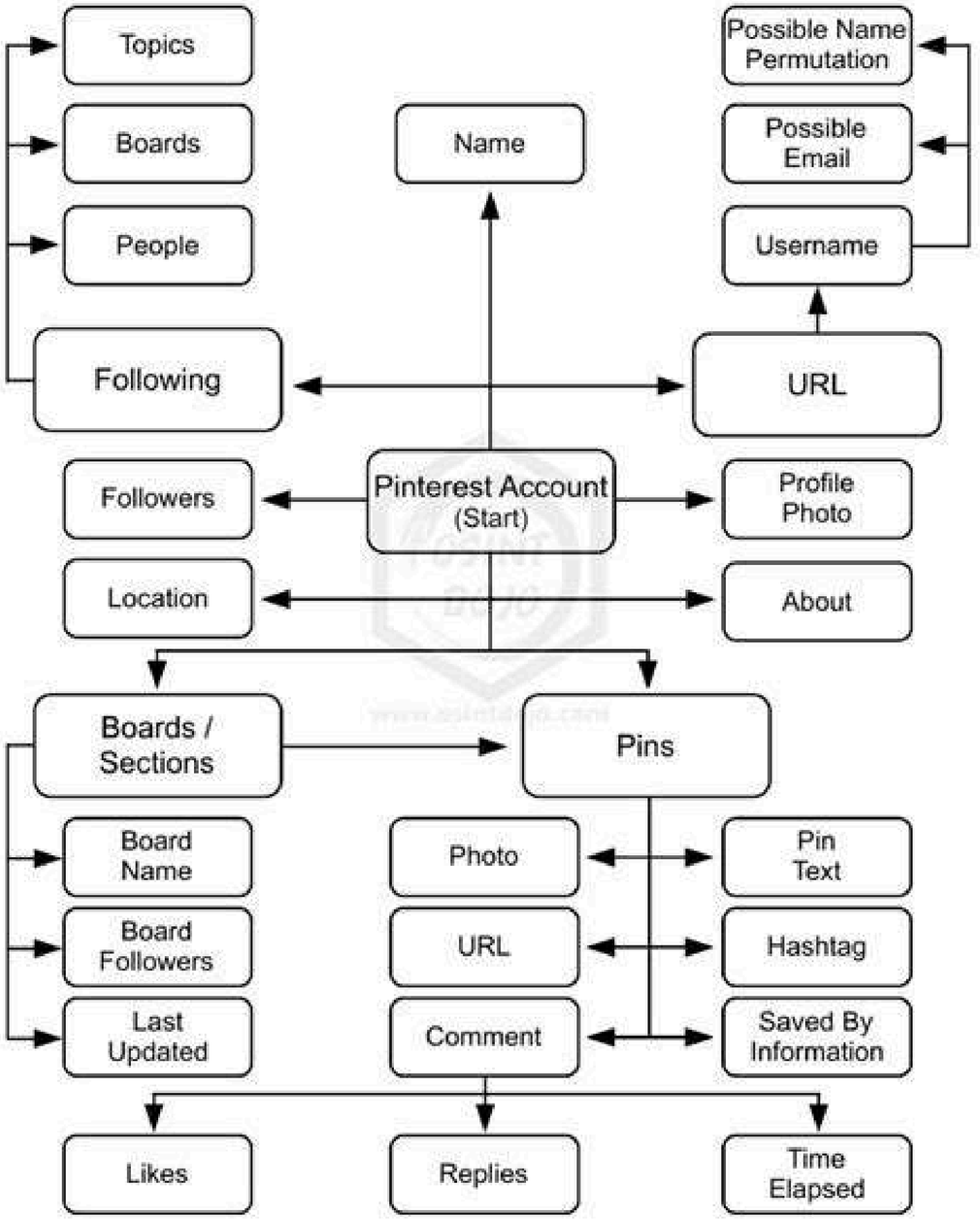
Telephone OSINT Tools – Truecaller, PhoneInfoga, NumVerify for call record analysis and telecom data leaks.



Vendor Osint

- Discusses Vendor OSINT, which involves tracking supply chains.
- Covers how competitor analysis relies on open-source intelligence.
- Highlights risks of corporate espionage via OSINT techniques.
- Suggests securing vendor contracts and supplier information.

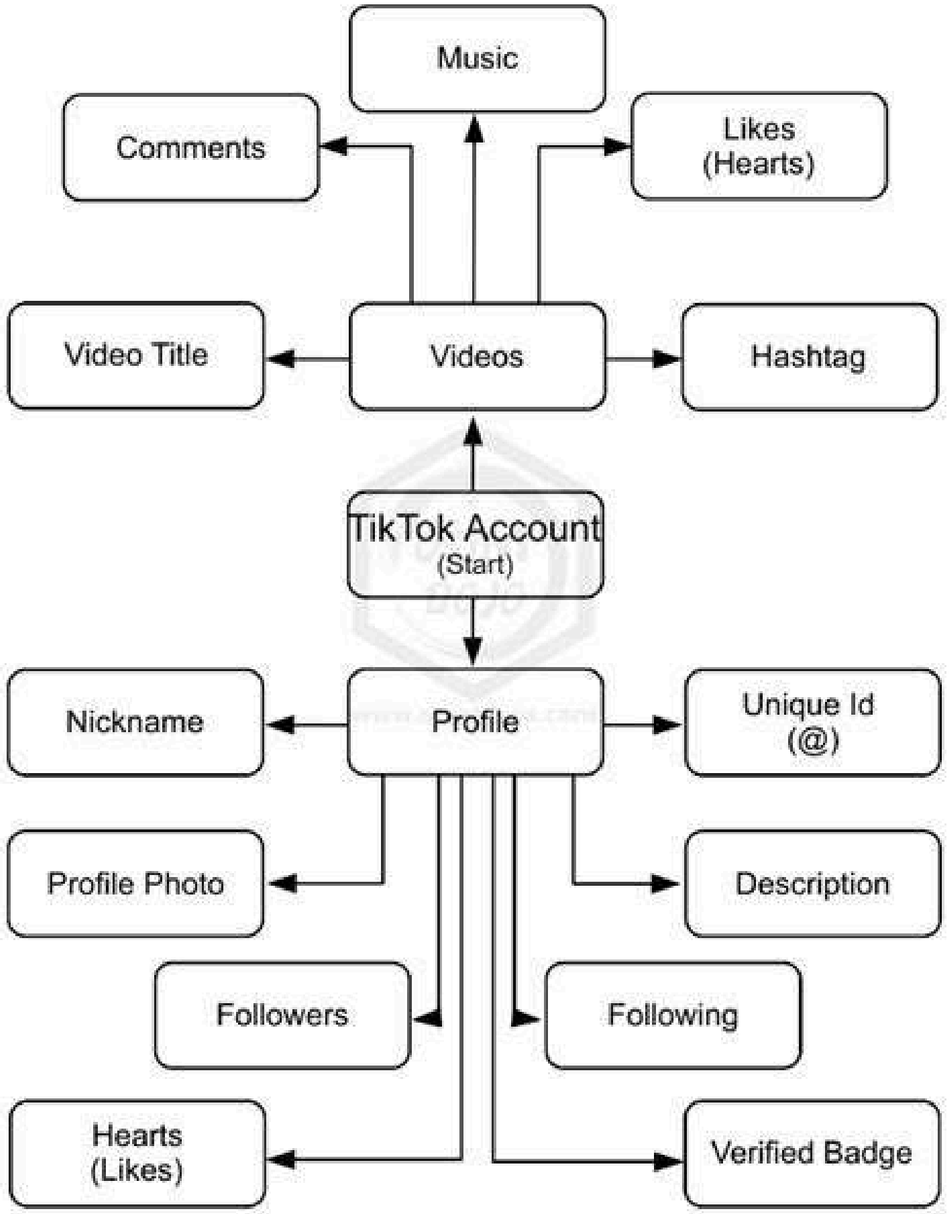
Vendor OSINT – Whois Lookup, BuiltWith for tracking supply chains and business intelligence



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.

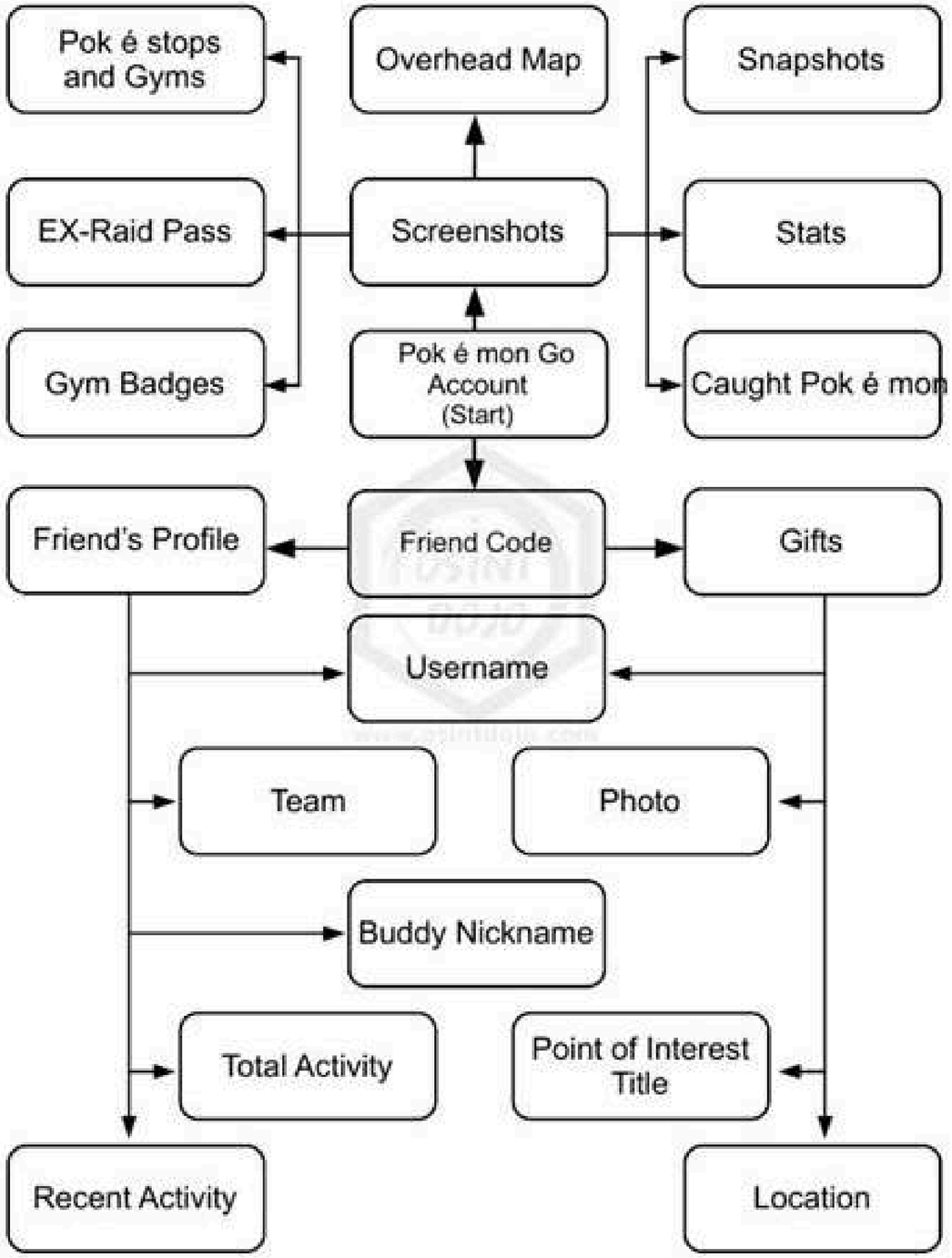
Pinterest OSINT Tools– Pinsearch, Image Reverse Search for tracking image metadata.



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.

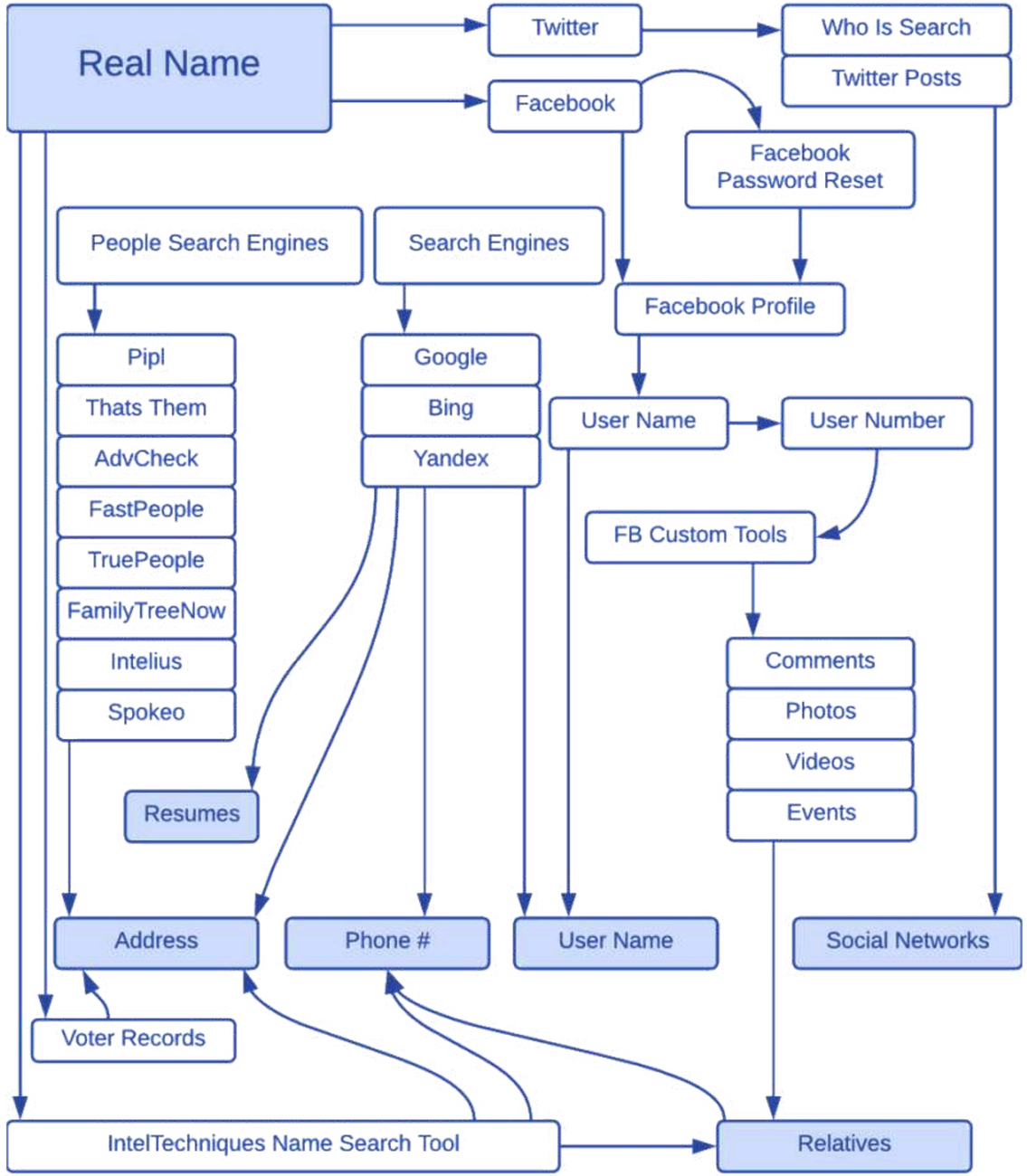
TikTok OSINT – OSINT Techniques, ExifTool, TikTok API monitoring for tracking user activities.



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.

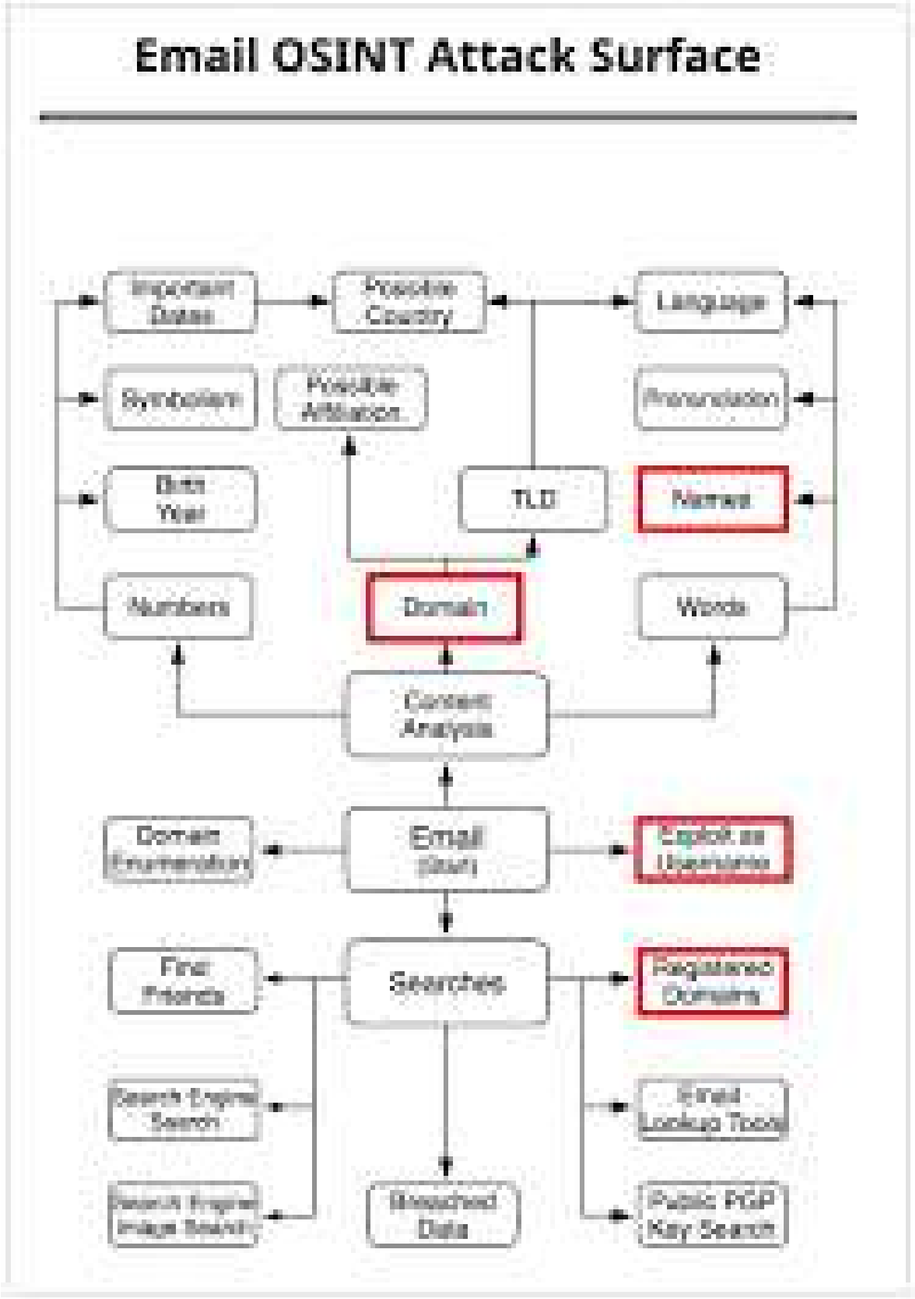
Pokémon Go OSINT Tools – PoGoMap, GPS Spoofing detection tools, location tracking via Pokémon Go logs.



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

- 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.

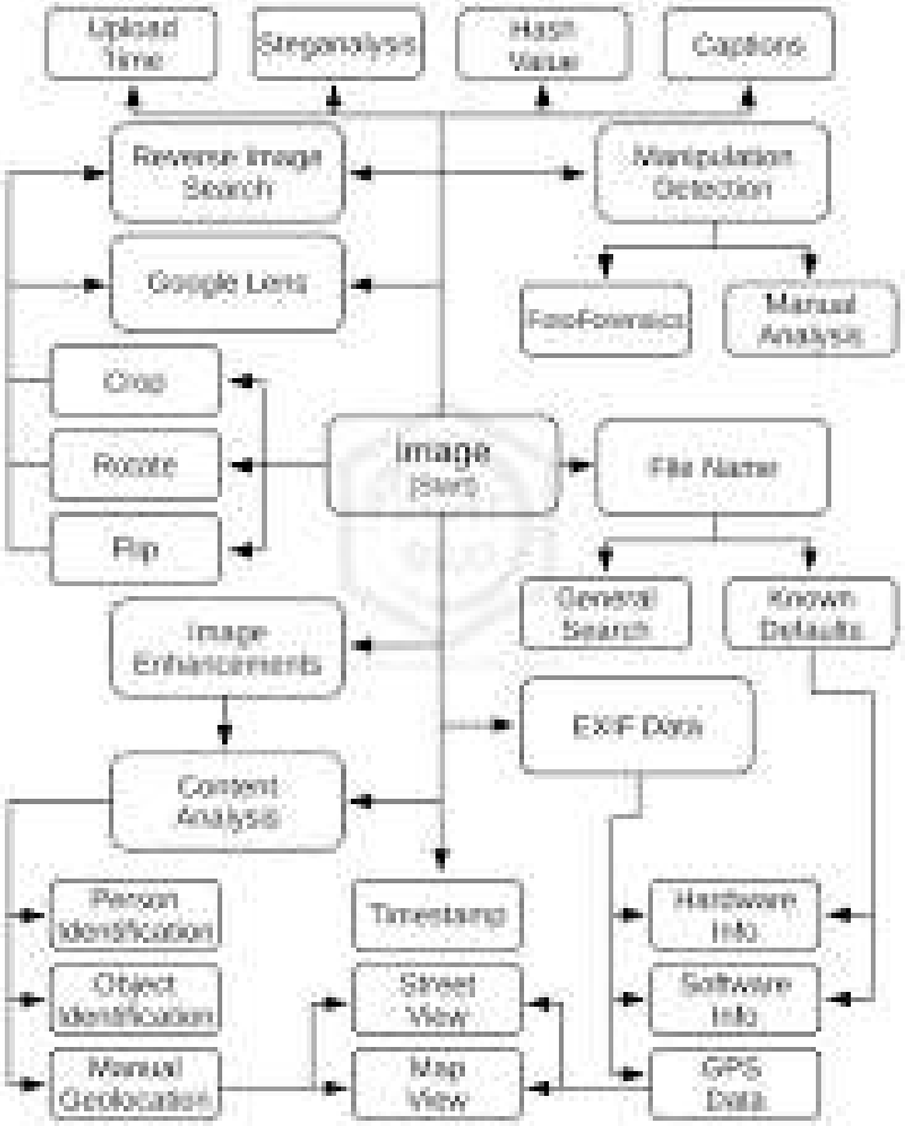
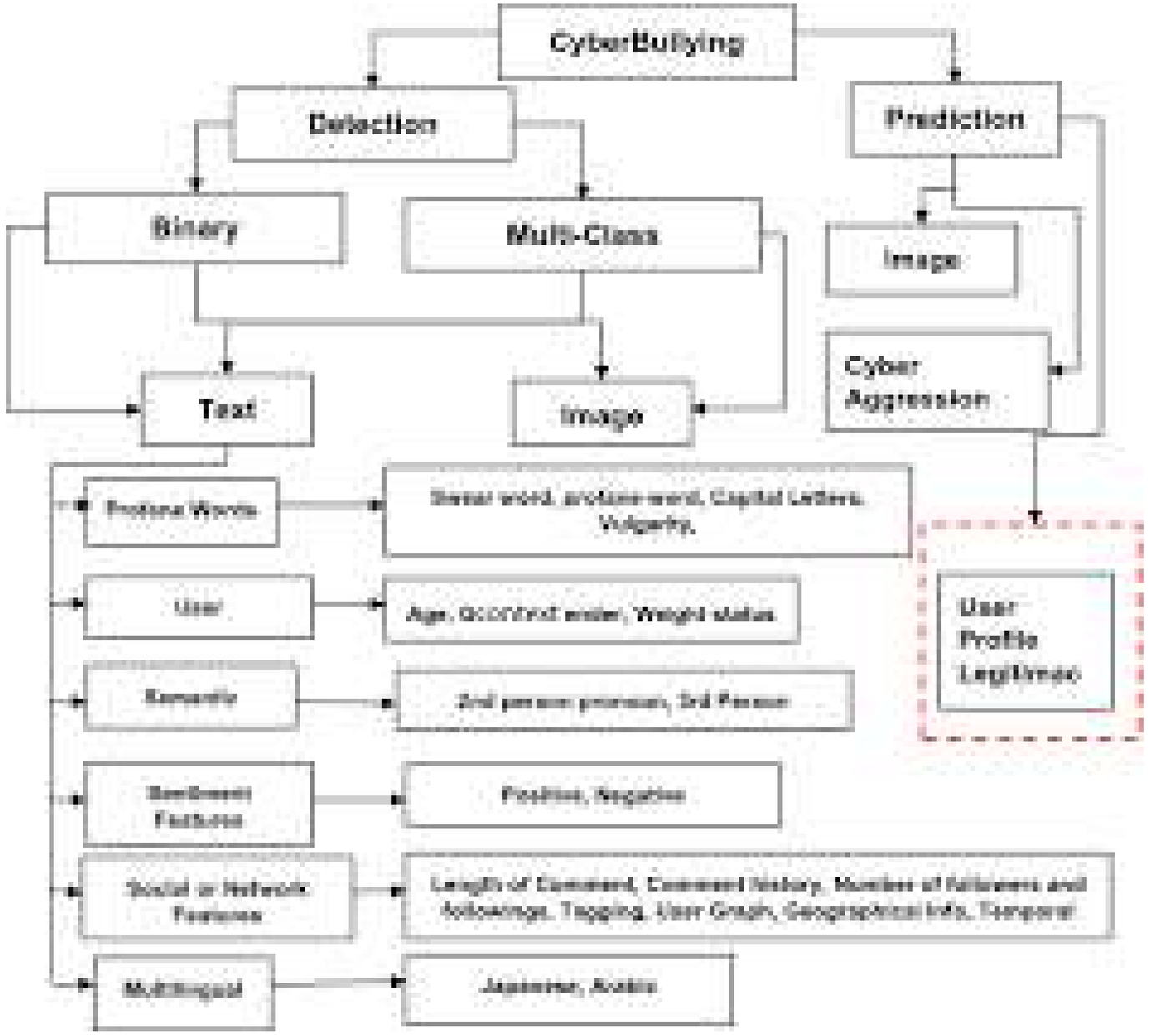
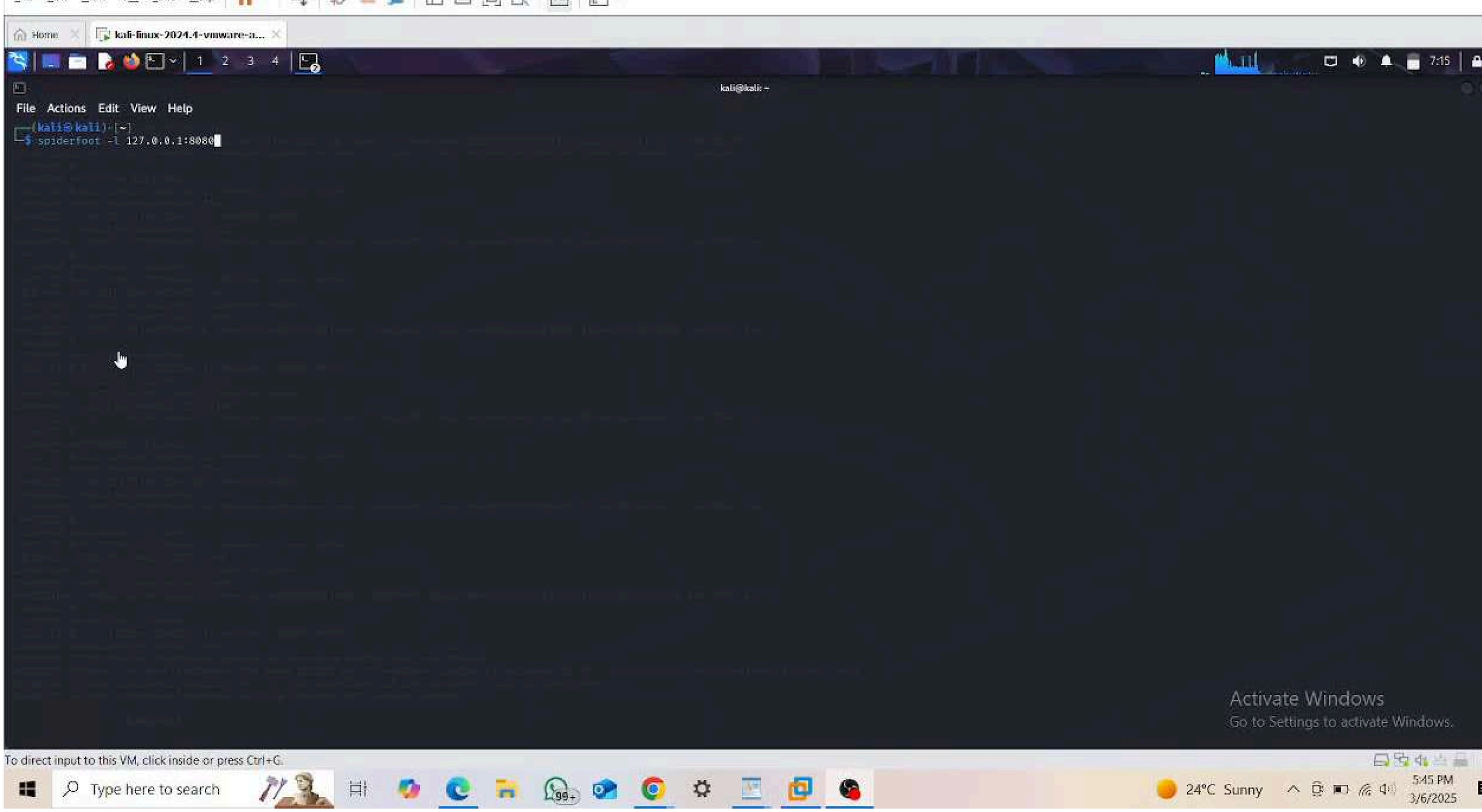


Image Osint

-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.


CyberBullying
Detection
Prediction
Binary
Multi-Class
Image
Text
Image
Cyber Aggression
Profane Words
Swear word, profane word, Capital Letters, Vulgarity,
User
Age, Gender, Weight status
User Profile Legitimac
Semantic
2nd person pronoun, 3rd Person
Sentiment Features
Positive, Negative
Social or Network Features
Length of Comment, Comment history, Number of followers and followings, Tagging, User Graph, Geographical Info, Temporal
Multilingual
Japanese, Arabic


Home
kali-linux-2024.4-vmware-a...
1 2 3 4
7:15
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ spiderfoot -l 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.
Type here to search
24°C Sunny
5:45 PM
3/6/2025


Thank You
Very Much!

Tools:-

@BreachHunter_Bot
@khoj
https://teleteg.com/
Google Earth Pro
https://epieos.com/

https://linktr.ee/digisur
?utm_source=linktre...