OSINT on X: How to Investigate Like a Pro

Administrator | 11/08/2025 | OSINT

The question every investigator asks is simple: *how much can you discover about a person or organization just from their presence on X?* The answer is—quite a lot. If you know the right techniques, the platform still offers a goldmine of data, even after its user numbers dipped following Elon Musk's takeover and rebranding in 2022. With over 335 million active users in 2024, X remains a real-time repository of opinions, connections, and location clues.

Why X Still Matters for OSINT

Even though it has lost millions of users compared to its 2023 peak, X continues to serve as a primary channel for breaking news, political discourse, and personal updates. For OSINT professionals, journalists, and analysts, the platform's value lies in the sheer immediacy of its content and the range of metadata attached to posts and profiles. This is where structured investigative methods can turn casual browsing into actionable intelligence.

Starting from the Profile

Every investigation on X begins with the profile page. An account has two names: the display name, which might be a real identity or an alias, and the username (or handle), which starts with "@" and is unique to the platform. Examining this page can yield a surprising amount of information. Profile and header images often appear on other platforms, sometimes under different names, while the short biography might contain links to personal websites, mentions of organizations, or hints about location.

The join date can give context to a user's activity history, while the followers and following lists are a starting point for mapping relationships. Even optional details such as date of birth or geographic location, if disclosed, can be significant. Checking whether a username appears on other social networks can reveal additional profiles, and reverse image searches can trace photographs back to other online presences.

Following the Clues Beyond the Platform

Links in a bio or post can lead to websites that open new investigative doors. A simple WHOIS lookup can reveal when a domain was registered, who owns it, and which hosting provider it uses. In some cases, archived versions of those sites, accessible via tools like the Wayback Machine or Archive.today, will contain older contact information, deleted job postings, or downloadable documents with metadata identifying authors and software used.

Technical analysis can also uncover patterns—multiple sites hosted on the same IP, or domains sharing Google Analytics codes, often indicate connections between projects or individuals. In OSINT, these subtle ties are where the most compelling leads emerge.

Searching Smarter on X

While the platform's basic search box is a good starting point, it quickly becomes limiting. The built-

in categories—Top, Latest, People, Media, and Lists—offer a way to segment results, but the real power comes from advanced search. This feature allows you to refine queries by specific words or phrases, language, account origin, engagement metrics, or a defined date range.

Instead of scrolling endlessly, you can, for example, search for posts in Arabic from a single account between two specific dates, or find all mentions of a topic that have attracted more than a certain number of likes.

The Language of Operators

Like Google, X responds to operators that make searches more precise. Adding filters such as from:username will limit results to a single account, while near:"city" and geocode:latitude,longitude,radius narrow them to a location. Media-specific searches—filter:images or filter:videos—can isolate visual content. By combining these elements, you can create highly targeted queries, such as finding English-language posts from a specific source that include a certain hashtag but exclude replies.

Extending the Search with Google Dorks

Sometimes the most revealing data isn't visible through X's interface at all. That's when Google Dorks come into play. By using search operators on Google, you can surface public content indexed outside the platform's own search. Queries like site:twitter.com intext:"data breach" or site:twitter.com inurl:lists intitle:"OSINT" allow you to pinpoint posts, lists, and conversations that the platform might not display directly.

Tools That Supercharge OSINT on X

Several external tools help push investigations further. Twint can scrape data from profiles without using the X API. Tweepy automates searches through the API itself. Mecodify offers data visualization and analysis, while network mapping tools like Gephi or NodeXL turn connections into clear visual graphs. For video or GIF extraction, specialized downloaders can preserve multimedia evidence before it disappears.

Keeping a Low Profile

All of these methods share one risk: being seen by your target. In social media intelligence (SOCMINT), it's easy to leave a trace—whether through "Who to Follow" algorithms or by showing up in viewed profile lists. That's why many professionals use managed attribution platforms such as Silo for Research, which mask identity and location while browsing.

The Takeaway

Investigating on X is part technical skill, part detective instinct. It means knowing how to move from a username to a web of connections, from a single image to a network of linked accounts, and from a casual post to a timeline of activity tied to a place.

The platform may have changed its name, ownership, and user base, but it remains a live feed of global human activity. For those who know how to navigate it, X is less a social network and more a dynamic database—one that's updated by the second.

STEP by STEP

Step 1: Understanding the Anatomy of an X Profile

Every X account has two names:

• Display Name – Could be a real name, nickname, or alias.

• Username (Handle) – Begins with “@” and is unique.

Other useful profile elements for OSINT:

• Profile & Header Images – Often reused across platforms.
• Bio – May contain links, affiliations, or location clues.
• Join Date – A potential indicator of account history.
• Followers/Following Lists – Network mapping gold.
• Location & Date of Birth (if public) – Geolocation and identity clues.

Pro Tip: Always check if the username appears on other platforms using tools like:

• Instant Username Search
• Maigret
• Sherlock

Step 2: Reverse Image and Bio Analysis

A profile picture isn’t just a photo — it’s a data point.

• Reverse Image Search Tools: Google Image Search
• Bing Visual Search
• PimEyes (facial recognition)
• Search4faces

Bio Clues:
Look for:
• Links to personal websites → run WHOIS lookups
• Mentions of organizations or hobbies → cross-check with public profiles
• Email addresses or usernames → plug into breach databases or OSINT tools

Step 3: Digging Deeper into Linked Websites

Many users link to personal or corporate sites. These can be exploited for:

• WHOIS History – Use Whoxy to track ownership changes.
• Shared Hosting – Find other sites on the same server with ViewDNS.
• Shared Analytics Codes – Use SpyOnWeb to discover related domains.

Archived versions from the **Wayback Machine** or **Archive.today** may reveal:

• Old contact details
• Deleted job postings
• Hidden PDFs with metadata

Step 4: Mastering X’s Built-in Search

The default search offers five categories:

• Top – Algorithmically relevant posts
• Latest – Chronological results
• People – Related accounts
• Media – Posts with images/videos

• Lists – Curated topic lists

Step 5: Advanced Search and Operators

The **Advanced Search** interface lets you filter by:

• Words & Phrases
• Specific Accounts
• Hashtags
• Language
• Engagement (likes, replies, reposts)
• Date Range

Key Search Operators:

• from:username – Posts from a specific account
• to:username – Replies to a specific account
• near:"city" – Posts near a city
• geocode:lat,long,radius – Precise location targeting
• filter:images / filter:videos – Media-specific posts
• Combine operators: sqlCopiaModifica#OSINT from:authentic8 filter:links -filter:replies lang:en

Step 6: Using Google Dorks for X

When X's search isn't enough, Google Dorks can dig deeper:

• site:twitter.com intext:"data breach"
• site:twitter.com inurl:status "zero-day exploit" after:2023
• site:twitter.com inurl:lists intitle:"OSINT" -inurl:members

Step 7: OSINT Tools for X

Boost your investigations with:

• Twint – Scrape data without the API.
• Tweepy – API-based search automation.
• Mecodify – Data analysis & visualization.
• NodeXL / Gephi – Network mapping tools.

Step 8: Operational Security (OPSEC)

When doing SOCMINT (Social Media Intelligence), you risk:

• Appearing in "Who to Follow" suggestions
• Alerting your target through profile views

Solution: Use a managed attribution platform like **Silo for Research** to mask your identity.
The question every investigator asks is simple: *how much can you discover about a person or organization just from their presence on X?* The answer is—quite a lot. If you know the right techniques, the platform still offers a goldmine of data, even after its user numbers dipped following Elon Musk's takeover and rebranding in 2022. With over 335 million active users in 2024, X remains a real-time repository of opinions, connections, and location clues.

Why X Still Matters for OSINT

Even though it has lost millions of users compared to its 2023 peak, X continues to serve as a primary channel for breaking news, political discourse, and personal updates. For OSINT professionals, journalists, and analysts, the platform’s value lies in the sheer immediacy of its content and the range of metadata attached to posts and profiles. This is where structured investigative methods can turn casual browsing into actionable intelligence.

Starting from the Profile

Every investigation on X begins with the profile page. An account has two names: the display name, which might be a real identity or an alias, and the username (or handle), which starts with “@” and is unique to the platform. Examining this page can yield a surprising amount of information. Profile and header images often appear on other platforms, sometimes under different names, while the short biography might contain links to personal websites, mentions of organizations, or hints about location.

The join date can give context to a user’s activity history, while the followers and following lists are a starting point for mapping relationships. Even optional details such as date of birth or geographic location, if disclosed, can be significant. Checking whether a username appears on other social networks can reveal additional profiles, and reverse image searches can trace photographs back to other online presences.

Following the Clues Beyond the Platform

Links in a bio or post can lead to websites that open new investigative doors. A simple WHOIS lookup can reveal when a domain was registered, who owns it, and which hosting provider it uses. In some cases, archived versions of those sites, accessible via tools like the Wayback Machine or Archive.today, will contain older contact information, deleted job postings, or downloadable documents with metadata identifying authors and software used.

Technical analysis can also uncover patterns—multiple sites hosted on the same IP, or domains sharing Google Analytics codes, often indicate connections between projects or individuals. In OSINT, these subtle ties are where the most compelling leads emerge.

Searching Smarter on X

While the platform’s basic search box is a good starting point, it quickly becomes limiting. The built-in categories—Top, Latest, People, Media, and Lists—offer a way to segment results, but the real power comes from advanced search. This feature allows you to refine queries by specific words or phrases, language, account origin, engagement metrics, or a defined date range.

Instead of scrolling endlessly, you can, for example, search for posts in Arabic from a single account between two specific dates, or find all mentions of a topic that have attracted more than a certain number of likes.

The Language of Operators

Like Google, X responds to operators that make searches more precise. Adding filters such as from:username will limit results to a single account, while near:"city" and geocode:latitude,longitude,radius narrow them to a location. Media-specific searches—filter:images or filter:videos—can isolate visual content. By combining these elements, you can create highly targeted queries, such as finding English-language posts from a specific source that include a certain hashtag but exclude replies.

Extending the Search with Google Dorks

Sometimes the most revealing data isn’t visible through X’s interface at all. That’s when Google Dorks come into play. By using search operators on Google, you can surface public content indexed outside the platform’s own search. Queries like site:twitter.com intext:"data breach" or site:twitter.com inurl:lists intitle:"OSINT" allow you to pinpoint posts, lists, and conversations that the platform might not display directly.

Tools That Supercharge OSINT on X

Several external tools help push investigations further. Twint can scrape data from profiles without using the X API. Tweepy automates searches through the API itself. Mecodify offers data visualization and analysis, while network mapping tools like Gephi or NodeXL turn connections into clear visual graphs. For video or GIF extraction, specialized downloaders can preserve multimedia evidence before it disappears.

Keeping a Low Profile

All of these methods share one risk: being seen by your target. In social media intelligence (SOCMINT), it’s easy to leave a trace—whether through “Who to Follow” algorithms or by showing up in viewed profile lists. That’s why many professionals use managed attribution platforms such as Silo for Research, which mask identity and location while browsing.

The Takeaway

Investigating on X is part technical skill, part detective instinct. It means knowing how to move from a username to a web of connections, from a single image to a network of linked accounts, and from a casual post to a timeline of activity tied to a place.

The platform may have changed its name, ownership, and user base, but it remains a live feed of global human activity. For those who know how to navigate it, X is less a social network and more a dynamic database—one that’s updated by the second.

STEP by STEP

Step 1: Understanding the Anatomy of an X Profile

Every X account has two names:

• Display Name – Could be a real name, nickname, or alias.
• Username (Handle) – Begins with “@” and is unique.

Other useful profile elements for OSINT:

• Profile & Header Images – Often reused across platforms.
• Bio – May contain links, affiliations, or location clues.
• Join Date – A potential indicator of account history.
• Followers/Following Lists – Network mapping gold.
• Location & Date of Birth (if public) – Geolocation and identity clues.

Pro Tip: Always check if the username appears on other platforms using tools like:

• Instant Username Search
• Maigret
• Sherlock

Step 2: Reverse Image and Bio Analysis

A profile picture isn’t just a photo — it’s a data point.

• Reverse Image Search Tools: Google Image Search
• Bing Visual Search
• PimEyes (facial recognition)
• Search4faces

Bio Clues:
Look for:
• Links to personal websites → run WHOIS lookups
• Mentions of organizations or hobbies → cross-check with public profiles
• Email addresses or usernames → plug into breach databases or OSINT tools

Step 3: Digging Deeper into Linked Websites

Many users link to personal or corporate sites. These can be exploited for:

• WHOIS History – Use Whoxy to track ownership changes.
• Shared Hosting – Find other sites on the same server with ViewDNS.
• Shared Analytics Codes – Use SpyOnWeb to discover related domains.

Archived versions from the **Wayback Machine** or **Archive.today** may reveal:

• Old contact details
• Deleted job postings
• Hidden PDFs with metadata

Step 4: Mastering X’s Built-in Search

The default search offers five categories:

• Top – Algorithmically relevant posts
• Latest – Chronological results
• People – Related accounts
• Media – Posts with images/videos
• Lists – Curated topic lists

Step 5: Advanced Search and Operators

The **Advanced Search** interface lets you filter by:

• Words & Phrases
• Specific Accounts
• Hashtags
• Language
• Engagement (likes, replies, reposts)
• Date Range

Key Search Operators:

• from:username – Posts from a specific account
• to:username – Replies to a specific account
• near:"city" – Posts near a city
• geocode:lat,long,radius – Precise location targeting

• filter:images / filter:videos – Media-specific posts
• Combine operators: sqlCopiaModifica#OSINT from:authentic8 filter:links -filter:replies lang:en

Step 6: Using Google Dorks for X

When X’s search isn’t enough, Google Dorks can dig deeper:

• site:twitter.com intext:"data breach"
• site:twitter.com inurl:status "zero-day exploit" after:2023
• site:twitter.com inurl:lists intitle:"OSINT" -inurl:members

Step 7: OSINT Tools for X

Boost your investigations with:

• Twint – Scrape data without the API.
• Tweepy – API-based search automation.
• Mecodify – Data analysis & visualization.
• NodeXL / Gephi – Network mapping tools.

Step 8: Operational Security (OPSEC)

When doing SOCMINT (Social Media Intelligence), you risk:

• Appearing in “Who to Follow” suggestions
• Alerting your target through profile views

Solution: Use a managed attribution platform like **Silo for Research** to mask your identity.