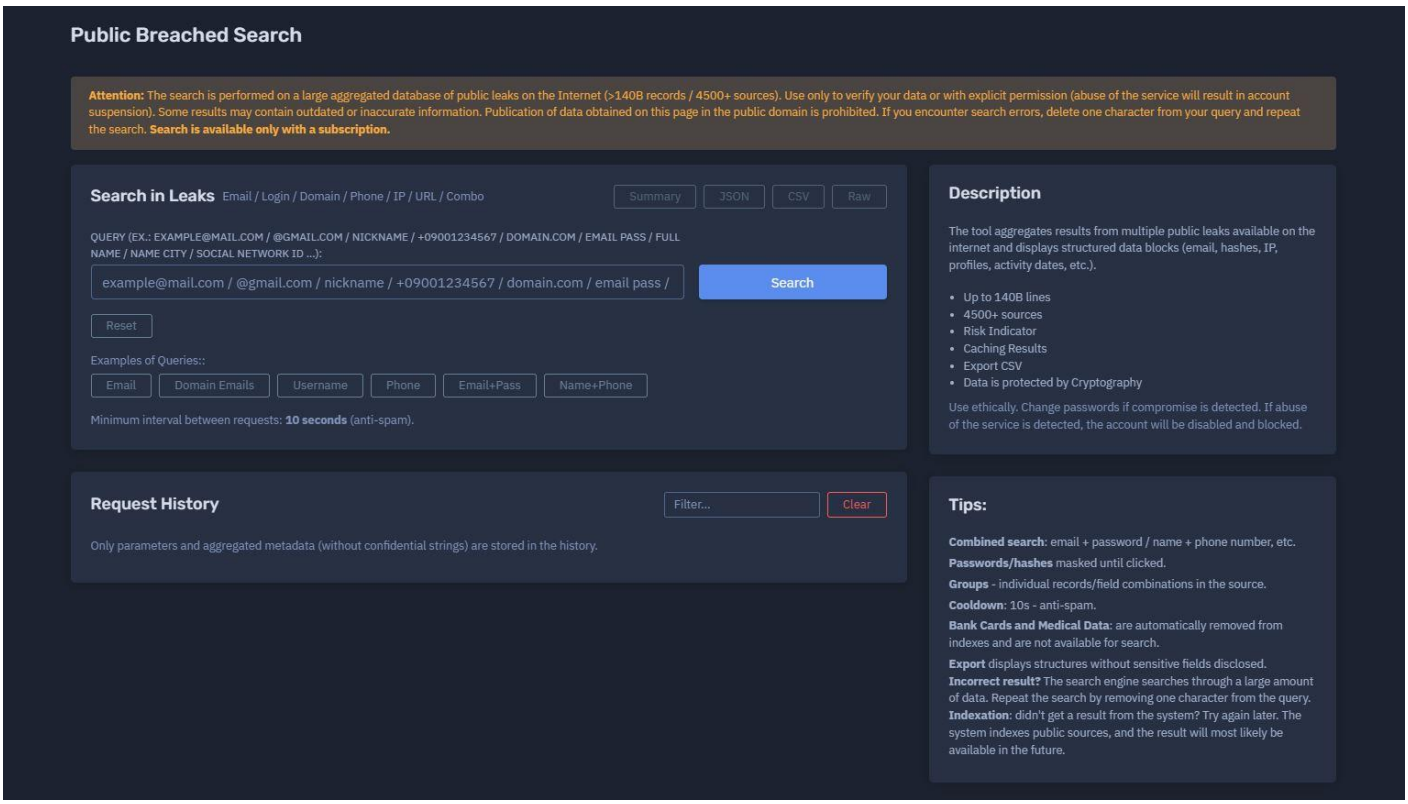
NiamonX Tools WiKi

NiamonX Tools WiKi is the central knowledge hub that provides detailed documentation, usage guides, and technical insights into all tools, modules, and research utilities developed within the **NiamonX ecosystem**.
It serves as a unified reference point for engineers, researchers, and security analysts working with NiamonX technologies in the fields of **AI, data intelligence, cybersecurity, and OSINT**.

Data Breach Search

Data Breach Search

Public Breached Search | Public Breaches (140+ Billion Records)



Overview of the Service

The platform available at **dash.niamonx.io/breaches_search** is a professional-grade **Public Breached Data Search System** designed for verifying whether specific personal identifiers have appeared in any known public data leaks across the Internet.
It operates on an **aggregated dataset exceeding 140 billion records** collected from **over 4,500 public breach sources**, making it one of the most extensive publicly searchable breach databases in existence.

? How the Search Works

When a user enters a query — such as an **email address, username, phone number, IP, or domain** — the system performs a real-time lookup across its encrypted, indexed data clusters. The query is normalized, tokenized, and securely matched against hashed or pseudonymized datasets to locate potential breach entries.

The search engine uses **multi-vector indexing** optimized for text, numeric, and composite keys (e.g., *email* + *password*, *name* + *city*), allowing flexible combined searches.

To maintain integrity and performance:

- Each user request is subject to a **10-second cooldown** (anti-spam policy).
- Partial queries can improve recall; deleting one character may trigger a broader match.
- Cached results are used for frequent queries to improve response time.

? What Can Be Searched

You can look up:

- **Emails and logins**
- **Phone numbers** (international format)
- **Domains or URLs**
- **IP addresses**
- **Full names or social network identifiers**
- **“Combo” lines** (e.g., *email* + *password* pairs from public leaks)

The system structures results into logical “groups” that may include:

- Email or login identifiers
- Hashed or masked passwords
- IP and domain references
- Profiles and related metadata
- First/last seen activity dates

Sensitive fields like passwords remain **masked** until explicitly revealed by the user.

?? Security & Ethics

All stored data and query logs are **encrypted using modern cryptographic algorithms**.
Only **aggregated metadata** — not full confidential strings — is retained in request history for transparency and analytics.

Additional safeguards:

- **Bank card and medical information** are automatically excluded from indexing.
- **Publication of retrieved data** is strictly forbidden.
- Detected abuse leads to **account suspension and IP blocking**.

The service is intended for **ethical use only** — such as checking whether your credentials or company assets appear in public leaks and taking appropriate security measures (e.g., password changes, MFA setup).

? Extra Features

- **Risk indicator:** assesses the exposure level of each result.
- **Result caching:** speeds up repeated lookups.
- **CSV export:** allows structured export without revealing sensitive fields.
- **Ongoing index updates:** new sources are continuously crawled and normalized.

In summary, **NiamonX Breach Search** acts as a secure, encrypted intelligence platform that enables professionals and individuals to verify their exposure in public breaches responsibly. It prioritizes **data protection, cryptographic integrity, and ethical transparency**, providing actionable insights while maintaining user and data privacy.

? Contact Information

For any inquiries, users can contact the project team directly:

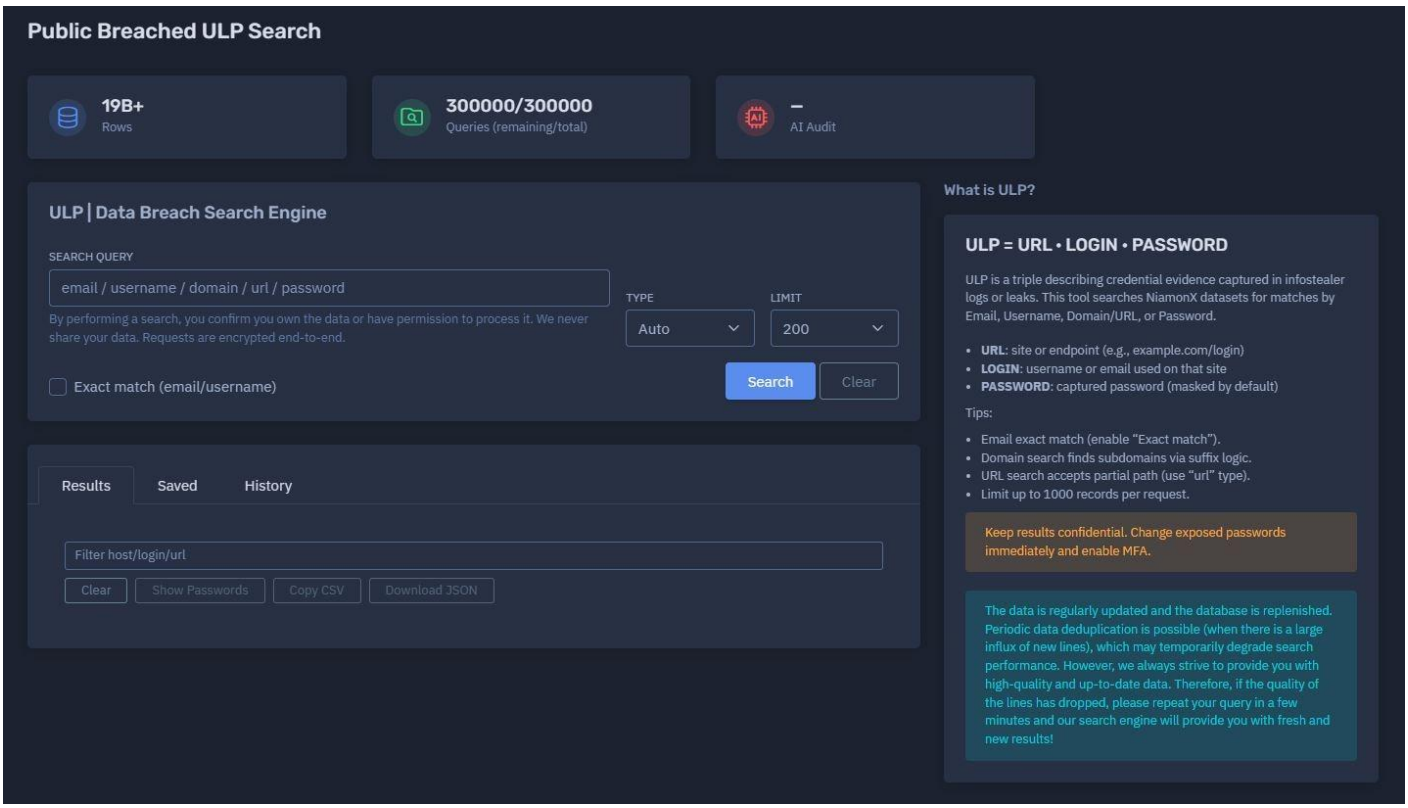
- **support @ niamonx.io** — Technical Support
- **other @ niamonx.io** — General Inquiries
- **takedown @ niamonx.io** — Requests for Data Removal / Privacy Takedowns
- **legal @ niamonx.io** — Legal Matters

An alternative contact channel is the official **Helpdesk**:

□□ https://support.niamonx.io/

Data Breach Search

ULP (Infostealer Logs) | Public Breached ULP Search



Overview of the Service

The platform available at **dash.niamonx.io/ulp_search** — known as **ULP Search** — is a specialized **Data Breach Search Engine** developed by **NiamonX** for identifying credential exposures in **public and infostealer leak datasets**.
It provides professionals and security researchers with a structured, secure, and ethical way to verify whether specific login credentials have been compromised online.

The ULP database currently indexes **over 19 billion credential records**, continuously updated and refined through automated pipelines, ensuring freshness, accuracy, and de-duplication.

? What is ULP?

ULP stands for **URL · LOGIN · PASSWORD**, representing a *credential triple* extracted from public or infostealer data sources.

Each record typically contains:

- **URL** — the website, endpoint, or domain where credentials were used (e.g., `example.com/login`)
- **LOGIN** — the associated username or email address
- **PASSWORD** — the captured or leaked password (masked by default for security)

This triplet allows correlation between breached accounts, reused passwords, and compromised domains, forming the foundation of forensic credential analysis within NiamonX's breach intelligence system.

? How the Search Works

Users can query the database using any of the following parameters:

- **Email address or username**
- **Domain or URL**
- **Password (masked matching supported)**

The system automatically detects the query type (`Auto` mode) or allows manual selection for more specific searches.
Searches are conducted in **real-time** against encrypted datasets, and results are filtered and ranked by confidence and relevance.

Key operational details:

- **Exact match** can be enabled for precise email or username lookups.
- **Domain-based searches** support suffix logic to detect subdomains (e.g., searching `example.com` will also include `mail.example.com`).
- **URL searches** accept partial paths, ideal for endpoint-level tracing.
- **Result limits:** up to 1,000 records per request.
- **Anti-abuse control:** all queries are encrypted and rate-limited.

If search performance temporarily decreases, it may indicate **active deduplication** or **dataset reindexing** — repeating the search after a few minutes ensures access to the freshest possible data.

? Key Features

- **AI Audit System:** enhances search precision and filters false positives through pattern-based validation and contextual AI analysis.
- **Result History & Filtering:** users can save searches, view historical queries, and filter by host, login, or URL.

- **Masked Passwords:** sensitive data remains hidden by default to prevent misuse.
- **Secure Export Options:** structured result exports with sensitive fields excluded.
- **Regular Updates:** continuous ingestion of verified breach data ensures up-to-date intelligence.

?? Security, Privacy & Ethics

Every search request is **fully encrypted end-to-end**, ensuring that user queries and results remain private.
The system never shares, resells, or exposes query data — even internally.

Ethical principles:

- Only perform searches for **data you own** or have **explicit authorization** to analyze.
- Keep results confidential and never redistribute them.
- Immediately **change any exposed passwords** and **enable multi-factor authentication (MFA)** if compromise is detected.
- Publication of retrieved data in open sources is strictly prohibited.

? Technical Highlights

- **19B+ credential records**
- **Real-time encrypted search**
- **Periodic deduplication & refresh cycles**
- **Adaptive caching for faster repeated queries**
- **Multi-type query engine (Email / Domain / URL / Password)**

? Contact Information

For support, inquiries, or privacy-related requests, the NiamonX team can be reached directly via:

- **support @ niamonx.io** — Technical Support
- **other @ niamonx.io** — General Inquiries
- **takedown @ niamonx.io** — Personal Data Removal Requests
- **legal @ niamonx.io** — Legal or Compliance Matters

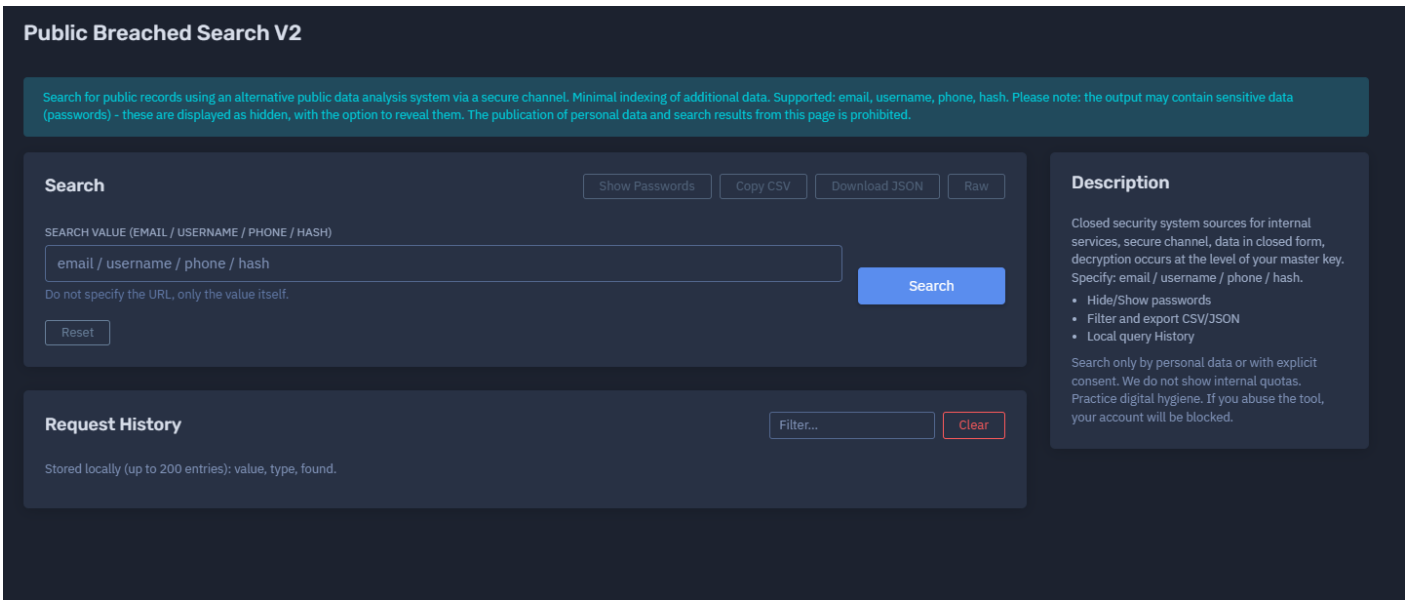
Alternative contact channel:

□□ **Helpdesk:** https://support.niamonx.io/

In summary, **NiamonX ULP Search** is a **cryptographically secure and ethically governed breach intelligence system** designed for professional credential analysis.
It provides deep visibility into compromised login data from billions of records — while maintaining the highest standards of **security, privacy, and responsible use**.

Data Breach Search

PBS v2 (Beta Search) | Public Breached Search V2



Overview of the Service

The platform available at dash.niamonx.io/breaches_s_v2 — known as **Public Breached Search V2** — is an advanced, security-focused version of the NiamonX breach intelligence engine. It enables users to safely and privately search for **publicly available leaked records** (emails, usernames, phone numbers, or hashes) through a **fully encrypted channel**, using an enhanced privacy-preserving architecture.

This system is designed for individuals, analysts, and cybersecurity teams who need to verify whether specific identifiers have been compromised — without exposing their search queries or retrieved data.

? How the Search Works

When a user submits a query — such as an **email address, username, phone number, or hash** — the system performs a real-time lookup across an **alternative, minimized index** of public breach data.
The search is executed through a **closed security network** using **end-to-end encryption** and a **master key–based decryption layer**. This ensures that:

- All transmitted data remains encrypted at every step.
- Decryption occurs **only on the client side**, not on NiamonX servers.
- The system never stores sensitive results or full identifiers in plain form.

This approach provides **maximum privacy**, ensuring that no third party — including NiamonX infrastructure — can access raw search data or results.

? What Can Be Searched

Supported input types:

- **Email address**
- **Username / Login**
- **Phone number** (international format)
- **Hash** (MD5 / SHA1 / SHA256 and similar)

Unlike the standard Breached Search engine, V2 does **not** support URLs, domains, or combined queries. It focuses exclusively on **personal identifiers and cryptographic hashes** to maintain precision and data hygiene.

Passwords found in results are **hidden (masked)** by default. Users may reveal them manually if needed for verification, but they must not redistribute or publicly display that information.

? Key Features

- **Encrypted Communication Channel:** every search request and response is transmitted securely.
- **Client-side Decryption:** sensitive content is decrypted locally using the user’s master key.
- **Minimal Indexing:** only essential metadata is stored to ensure fast lookups while reducing exposure.
- **Local Query History:** recent searches (up to 200 entries) are stored locally in the browser, not on the server.
- **Flexible Export:** results can be exported in **CSV** or **JSON** format, excluding confidential fields.
- **Password Visibility Control:** toggle to hide or show masked password fields.
- **Filtering System:** refine results by data type or source metadata.

?? Security, Privacy & Ethics

The service is built with **security-first architecture** and strict privacy guarantees:

- All communication is conducted through a **secure, encrypted channel**.
- Data is stored and processed in a **closed system** environment.
- **No internal quotas or usage metrics** are publicly displayed to prevent misuse.
- Searches must only be performed on **your own data** or with **explicit permission**.
- Abuse or attempts to deanonymize datasets will result in **account termination**.
- **Publication of personal or sensitive data retrieved from the system is strictly forbidden.**

Users are strongly encouraged to **practice digital hygiene** — for example, by changing passwords, enabling MFA, and avoiding credential reuse.

?? Technical Highlights

- **Alternative breach dataset with minimal indexing**
- **Closed internal security infrastructure**
- **End-to-end encryption with client-side decryption**
- **Local storage of query history (no server retention)**
- **Supports: email / username / phone / hash**
- **Output masking for passwords and sensitive fields**
- **CSV/JSON export with filtering tools**

? Contact Information

For any technical, legal, or privacy-related inquiries, users can reach the NiamonX team directly via:

- **support @ niamonx.io** — Technical Support
- **other @ niamonx.io** — General Inquiries
- **takedown @ niamonx.io** — Requests for Data Removal / Privacy Takedowns
- **legal @ niamonx.io** — Legal or Compliance Matters

Alternative contact channel:

□□ **Helpdesk:** https://support.niamonx.io/

In summary, **NiamonX Public Breached Search V2** is a **secure, privacy-preserving intelligence system** that enables safe and encrypted lookup of breach data.
It prioritizes **user confidentiality, cryptographic protection, and ethical operation**, ensuring that every search remains private, traceable only to the authorized user, and never exposed beyond their secure session.

OSINT Tools

OSINT Tools

Visual Osint (FotoForensics / ExifTool / Risk Score)

Overview of the Service

The **Visual OSINT** module — available as part of the NiamonX investigation suite — is an advanced **photo forensics and metadata analysis tool** that helps identify image manipulation, origin, and authenticity indicators.
It integrates multiple forensic technologies — including **FotoForensics-style artifact analysis**, **ExifTool-based metadata extraction**, and **CASIA AI prediction** — to deliver a complete visual intelligence assessment for investigators, journalists, and security analysts.

? What the Tool Does

Visual OSINT performs a deep, server-side forensic analysis of uploaded images, combining pixel-level inspection, metadata parsing, and AI-driven anomaly detection.

Supported file types: **JPEG, PNG, WebP** (up to 25 MB).
Each file is securely uploaded to NiamonX’s processing server, analyzed through a FotoForensics-

like API, and returned with visual and statistical breakdowns.

The system enforces a **cooldown of 30 seconds per request** and allows up to **90 seconds for processing**.

? Core Analysis Features

1. **Image Forensics (Visual Analysis)**
   The tool generates multiple forensic artifacts and comparisons:
   - **Original / Compressed Copy**
   - **Diff & Amplified Diff** (highlights pixel-level differences)
   - **Overlay & Artifact Grid** (visualizes edited regions)
   - **ELA (Error Level Analysis)** — identifies compression and tampering zones
   - **Noise Map** — isolates sensor and noise inconsistencies
   - **CASIA Prediction** — AI model inference from CASIA dataset to detect manipulation patterns
2. **EXIF & Metadata Extraction**
   Metadata is extracted using **PHP EXIF and ExifTool** modules, including:
   - Camera and software data
   - Creation timestamps
   - GPS coordinates (if embedded)
   - Editing traces and unusual tags
   - Hidden text or string data (binary text extraction)
3. **String Analysis**
   The tool detects **embedded ASCII or Unicode strings**, sometimes hidden within images.
   Long strings can indicate **metadata injection** or **hidden payloads**.
4. **GPS & Geolocation**
   If available, GPS coordinates are extracted and highlighted for quick mapping or cross-verification.

?? Risk Score System

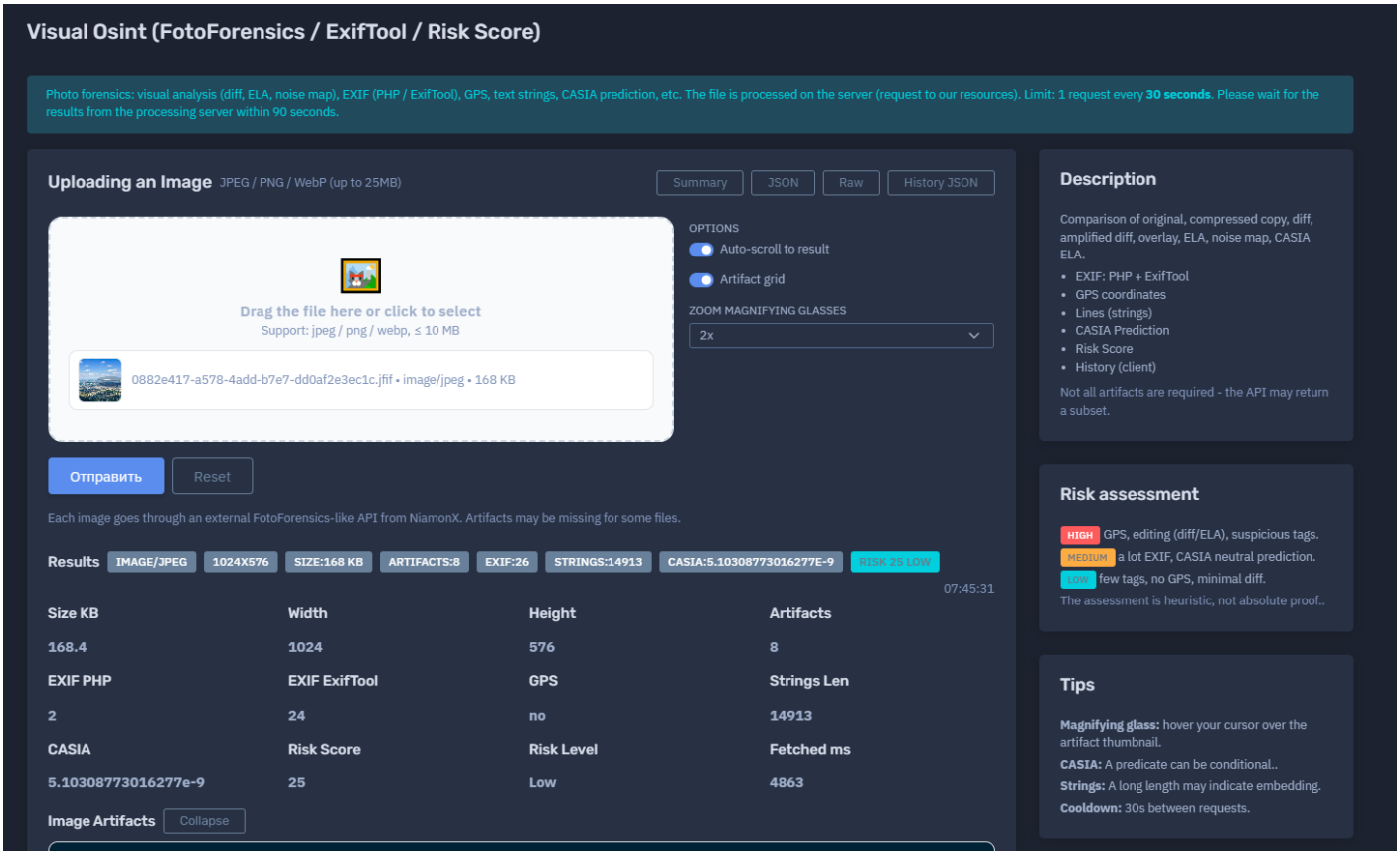
Each image receives a **heuristic Risk Score**, assessing the likelihood of manipulation or sensitive content presence:

- **High Risk:**
  GPS data present, strong ELA/diff indicators, suspicious or inconsistent tags.
- **Medium Risk:**
  Rich EXIF metadata, CASIA neutral or borderline prediction, potential editing hints.
- **Low Risk:**
  Minimal tags, no GPS, stable compression, and no visible tampering evidence.

> ⚠ The score is **heuristic** — not absolute proof — and should be interpreted as an analytical indicator rather than forensic certification.

? Tips for Use

- Hover the mouse over **artifact thumbnails** to use the built-in **magnifying glass (4x zoom)**.
- Enable **auto-scroll** to jump to results automatically after processing.
- Some files may return **partial artifacts** depending on compression level or EXIF structure.
- Long embedded strings or missing ELA layers can be signals of **steganography** or **format re-encoding**.



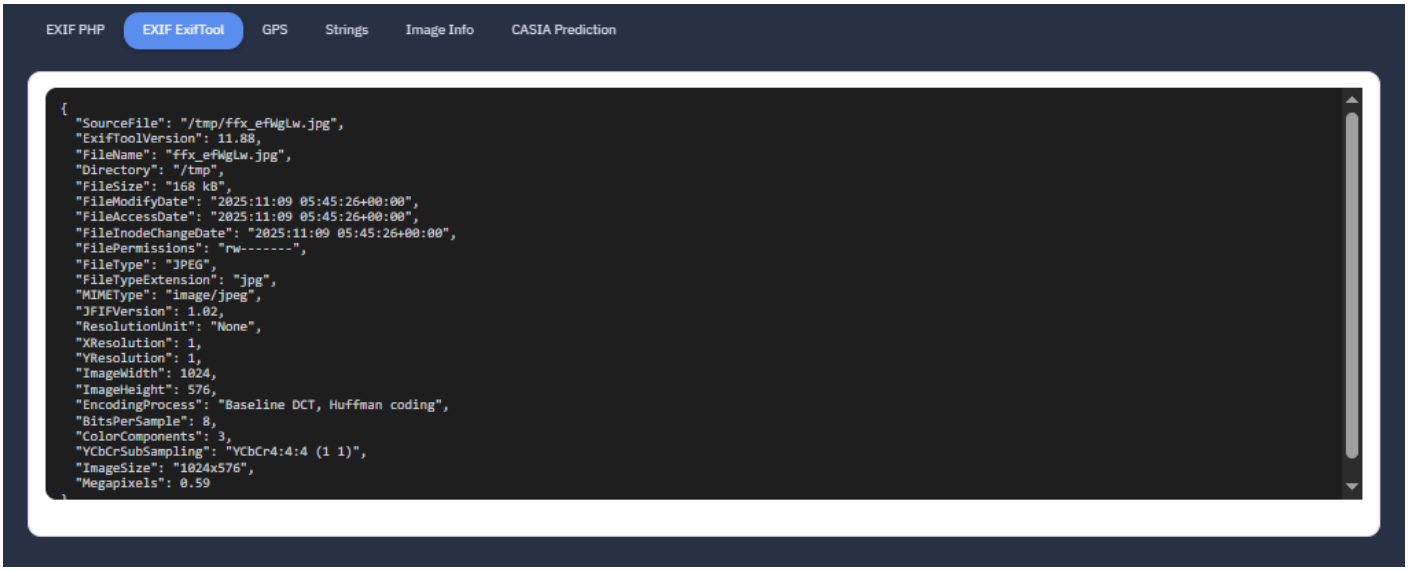
? Request History

- Stored **locally only** (up to 50 entries).
- Records include: filename, file size, GPS presence, calculated risk score, and main detected features.
- No data or images are stored on NiamonX servers after processing completion.

?? Security & Privacy

All image uploads and forensic analyses are processed via **secure, encrypted channels**.
The service never retains or shares the uploaded files or results.
Each request is isolated and deleted after processing to maintain strict **data confidentiality** and **user privacy**.

Users are encouraged to perform analyses only on **legally obtained images** and to respect privacy and consent regulations when handling visual materials.



? Contact Information

For inquiries, assistance, or data-related requests, contact the NiamonX team:

- **support @ niamonx.io** — Technical Support
- **other @ niamonx.io** — General Questions
- **takedown @ niamonx.io** — Requests for Data Removal / Privacy Takedowns
- **legal @ niamonx.io** — Legal or Compliance Matters

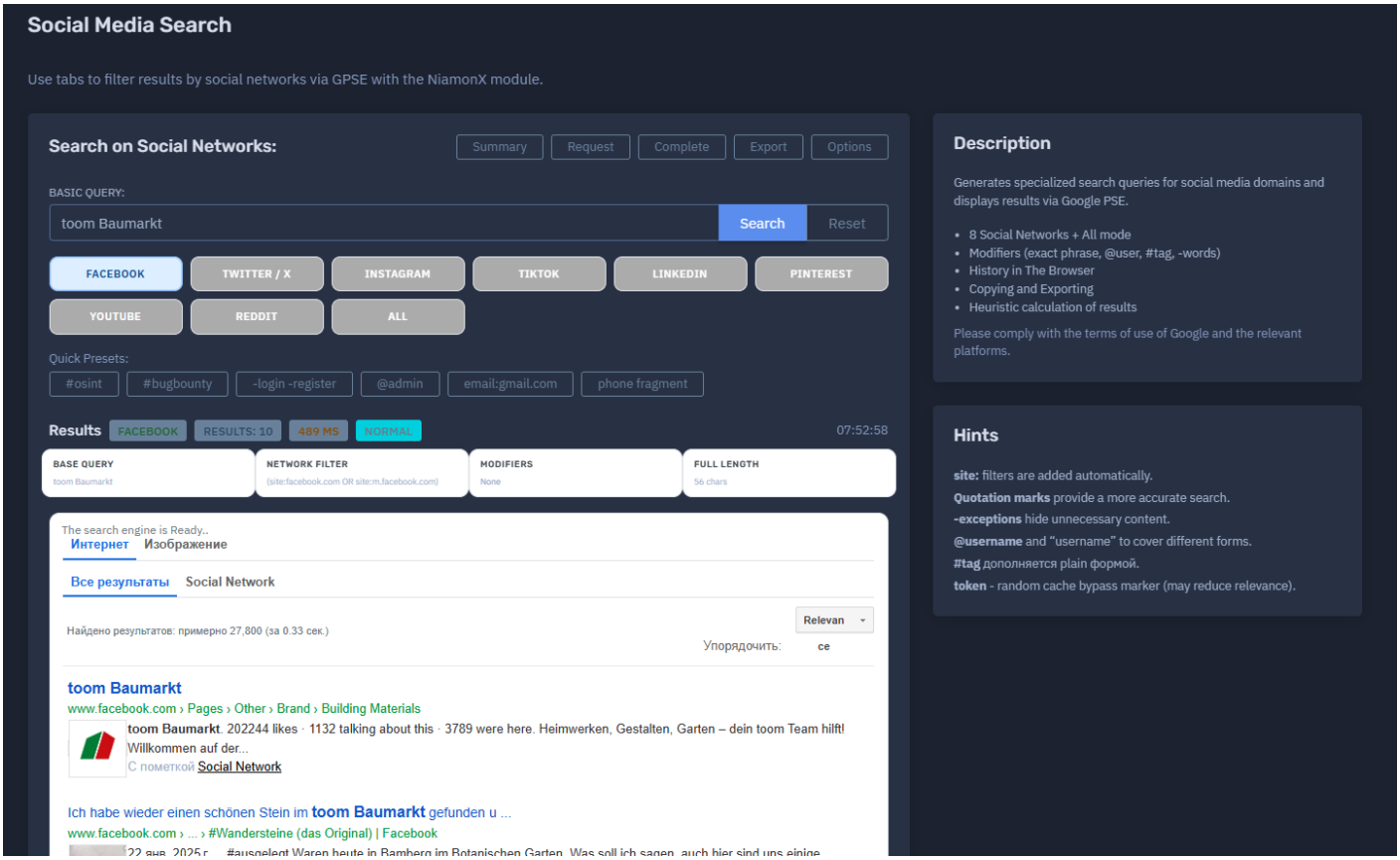
Alternative contact channel:

□□ **Helpdesk:** https://support.niamonx.io/

In summary, **NiamonX Visual OSINT** is a **comprehensive image forensics platform** combining traditional EXIF metadata inspection, advanced artifact visualization, and AI-driven manipulation detection.
It provides investigators with reliable insights into image authenticity and integrity — while maintaining the highest standards of **security, privacy, and digital ethics**.

OSINT Tools

Social Media Search



Social Media Search — NiamonX

Link: https://dash.niamonx.io/social_msearch

What it is

The Social Media Search tool is a focused OSINT utility that generates and runs specialized search queries across social media domains using **Google Programmable Search Engine (GPSE)** combined with NiamonX query logic. It helps investigators, analysts, and researchers locate public social footprints quickly by applying network-specific filters, modifiers and heuristics — without scraping protected APIs.

Key functionality

- **Tab-based network filtering:** Switch between tabs for individual social networks (8 supported networks) or run in **All** mode to cover multiple platforms at once.
- **Query types supported:** username, email, keywords, hashtags, mentions, and free-text phrases.
- **Smart query generation:** The interface auto-builds site: and domain-specific queries for each social network using GPSE and NiamonX heuristics.
- **Modifiers & presets:** Use exact-phrase (`"..."`), `@user`, `#tag`, `-excludedword` and other modifiers to refine results. Quick presets speed up common searches.
- **Heuristic scoring:** Results are scored/filtered by a heuristic engine that highlights higher-probability matches (based on signal strength, domain match, recency and pattern matching).
- **History & local storage:** Recent queries are stored locally in the browser (history, filters) for convenience — nothing is pushed to public indexes by the tool itself.
- **Copying & export:** Ability to copy results and export structured lists for reporting or follow-up analysis.
- **Token parameter:** An optional random token parameter can be appended to bypass aggressive caching (note: may reduce relevance).

How the search works (high level)

1. You enter a basic query (username, email, keywords).
2. NiamonX constructs network-aware GPSE queries (site:facebook.com “username”, site:twitter.com @user, etc.) and applies modifiers you selected.
3. GPSE executes the search and returns results; NiamonX post-processes them with heuristic filters and presents ranked results in the UI.
4. You can switch tabs to view results restricted to a given social domain or view aggregated results in All mode.

Because the tool relies on Google’s index, results depend on what Google has crawled and indexed for each social network.

What you can search for

- Public profiles by **username** or handle.
- Mentions or posts containing **emails** or **keywords**.
- **Hashtags** and topical content (`#tag`).
- **Exact phrases** (use quotes) and exclusion filters (`-word`).
- Quick multi-network scans (All mode) for footprint discovery.

Limitations & important notes

- **Depends on Google index:** not a replacement for direct API access to private or rate-limited platform data. If something isn't on Google, the tool won't find it.
- **No protected-data access:** does not access private profiles or bypass platform protections.
- **Token cache-bypass:** using the random token can force fresher Google results but may lower result relevance.
- **Respect platform TOS:** you must comply with Google's and target platforms' terms of service. Abuse may result in blocked access.
- **Local history only:** history is kept in the browser (not shared publicly); sensitive searches should be handled carefully.

Best-practice tips

- Use quotation marks for exact phrase matches.
- Combine `@username` and `"username"` to cover different forms and variations.
- Use `-word` to remove noisy sources from results.
- Try All mode first for broad reconnaissance, then switch to a specific network tab to drill down.
- If results look stale, re-run the query or tweak modifiers (Google index freshness varies).

Privacy & security

- The tool generates queries and shows results via GPSE; it does **not** harvest private data or bypass access controls.
- Query history resides in the user's browser. NiamonX post-processing applies heuristics but does not expose private platform data.
- Use the tool only for lawful, authorized investigations and with respect for privacy.

Contact / support

For any questions, reporting issues, or compliance requests, contact the NiamonX team:

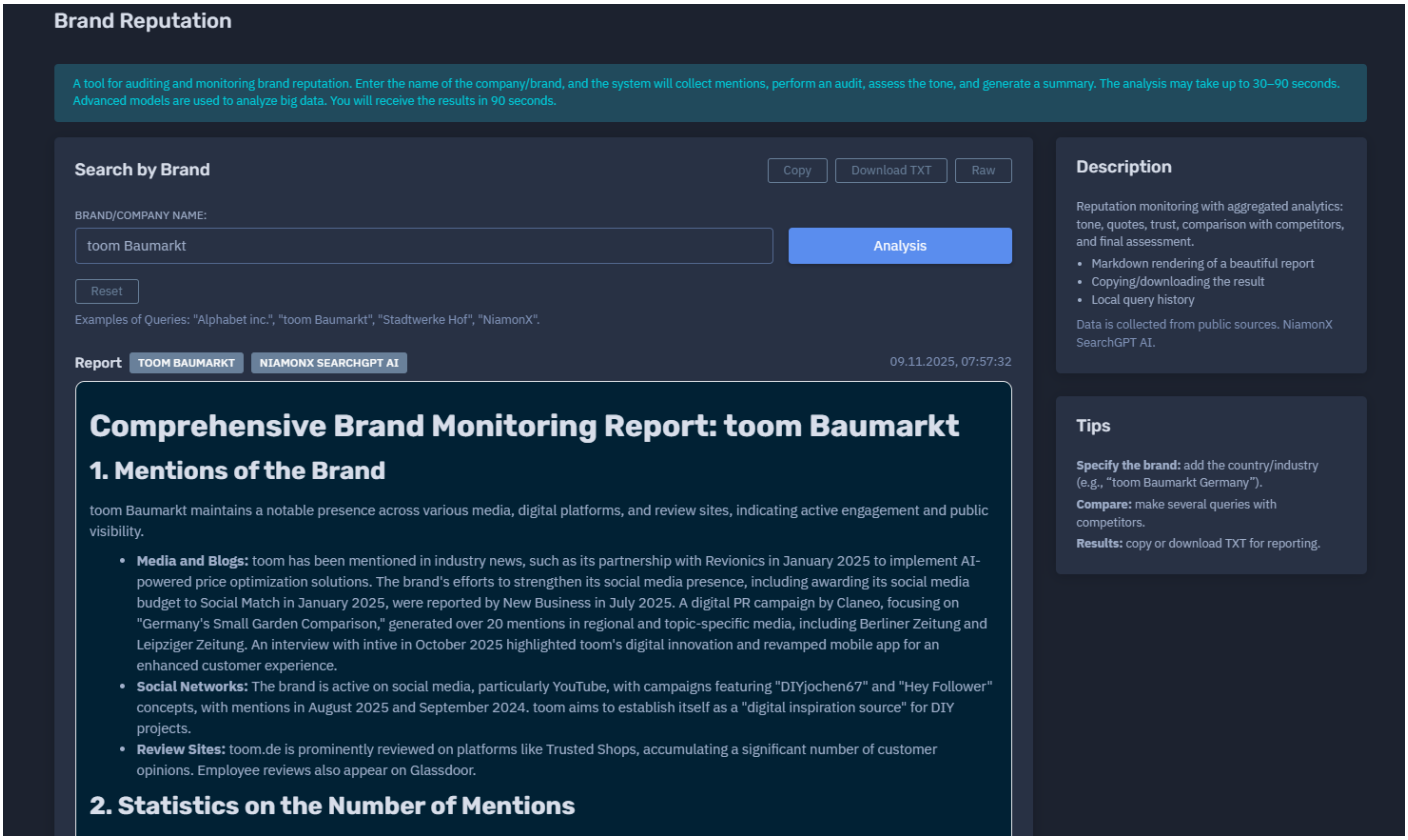
- **support @ niamonx.io** — Technical Support

- **other @ niamonx.io** — General Inquiries
- **takedown @ niamonx.io** — Data removal / privacy takedowns
- **legal @ niamonx.io** — Legal / compliance

Alternative channel: **Helpdesk** → https://support.niamonx.io/

OSINT Tools

Brand Reputation



Brand Reputation — NiamonX

Link: https://dash.niamonx.io/brand_reputation

What it is
The **Brand Reputation** module is a next-generation AI-powered system for **brand perception auditing, sentiment tracking, and trust assessment**. It automatically gathers and analyzes public mentions of any company or brand name, evaluates overall tone and credibility, and generates a structured analytical report in under 90 seconds.

Built on top of **NiamonX SearchGPT AI**, it processes large datasets from multiple open sources, performing sentiment analysis, contextual clustering, and reputation scoring — all securely and locally processed with end-to-end encryption.

Key Functionality

- **Automated Brand Intelligence:** Enter a brand or company name; the system collects public mentions from online sources and performs semantic tone analysis.
- **Tone and Sentiment Detection:** Determines whether general sentiment is positive, neutral, or negative across aggregated mentions.
- **Trust and Risk Analysis:** Evaluates credibility of sources, consistency of tone, and potential risks to brand trust.
- **Comparative Analysis:** Allows comparing your brand's score with competitors (e.g., "toom Baumarkt Germany" vs. "OBI Germany").
- **Comprehensive Report Generation:** Produces a Markdown-formatted summary with sections for tone overview, key quotes, trends, competitor metrics, and final evaluation.
- **Local Query History:** Stores up to 200 recent searches locally (brand names and short previews only — no personal or external data).
- **Copy & Download Options:** Instantly copy or export the report in `.txt` format for presentations or documentation.

How It Works

1. You enter a **brand or company name** (e.g., "Alphabet Inc." or "NiamonX").
2. The engine collects relevant mentions from public data sources.
3. NiamonX AI performs a **multi-layer audit**: text clustering, tone detection, quote extraction, and trust scoring.
4. Within **30–90 seconds**, you receive a detailed Markdown report summarizing findings with sentiment breakdown, trend indicators, and confidence ratings.

What You Can Analyze

- **Corporate and consumer brands** (e.g., "IKEA", "Tesla", "Lufthansa").
- **Institutions or municipalities** (e.g., "Stadtwerke Hof").
- **Startups and emerging brands** (e.g., "NiamonX").
- **Cross-regional or industry-specific brands** ("toom Baumarkt Germany", "Volksbank Berlin").

Report Contents

- **Summary Overview** — concise snapshot of brand tone and reputation level.

- **Tone Analysis** — positive, neutral, negative tone distribution with percentages.
- **Quotes & Mentions** — key extracted phrases and examples.
- **Trust & Source Evaluation** — assessment of data credibility and bias level.
- **Competitor Comparison** — optional comparison with rival brands.
- **Final Assessment** — heuristic reputation score from 0–100 (aggregated).

Markdown rendering ensures each report is **visually clear, structured, and ready for presentation**.

Privacy & Security

- Data is **collected only from public sources** — no hidden APIs or unauthorized data scraping.
- All queries and results are processed through a **secure encrypted channel**.
- Local browser storage is used for history; no external telemetry or analytics.
- Generated reports are transient — not shared or indexed anywhere.

Tips for Best Results

- Add **geographical or industry context** to the query (e.g., “toom Baumarkt Germany”, “Airbus Aerospace”).
- Compare **multiple competitors** for benchmarking.
- Export results as `.txt` or copy Markdown directly into reports.
- Wait the full 90 seconds for the analysis to complete; large datasets require deep semantic evaluation.

Example Use Cases

- **PR & Marketing Teams:** Track brand health, press tone, and audience sentiment.
- **Corporate Analysts:** Monitor changes in brand perception or response to public events.
- **Investors:** Assess brand stability and public trust before funding decisions.
- **Reputation Management Firms:** Automate large-scale audits using AI-based contextual scoring.

Contact / Support

For issues, assistance, or legal inquiries:

Helpdesk: https://support.niamonx.io