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

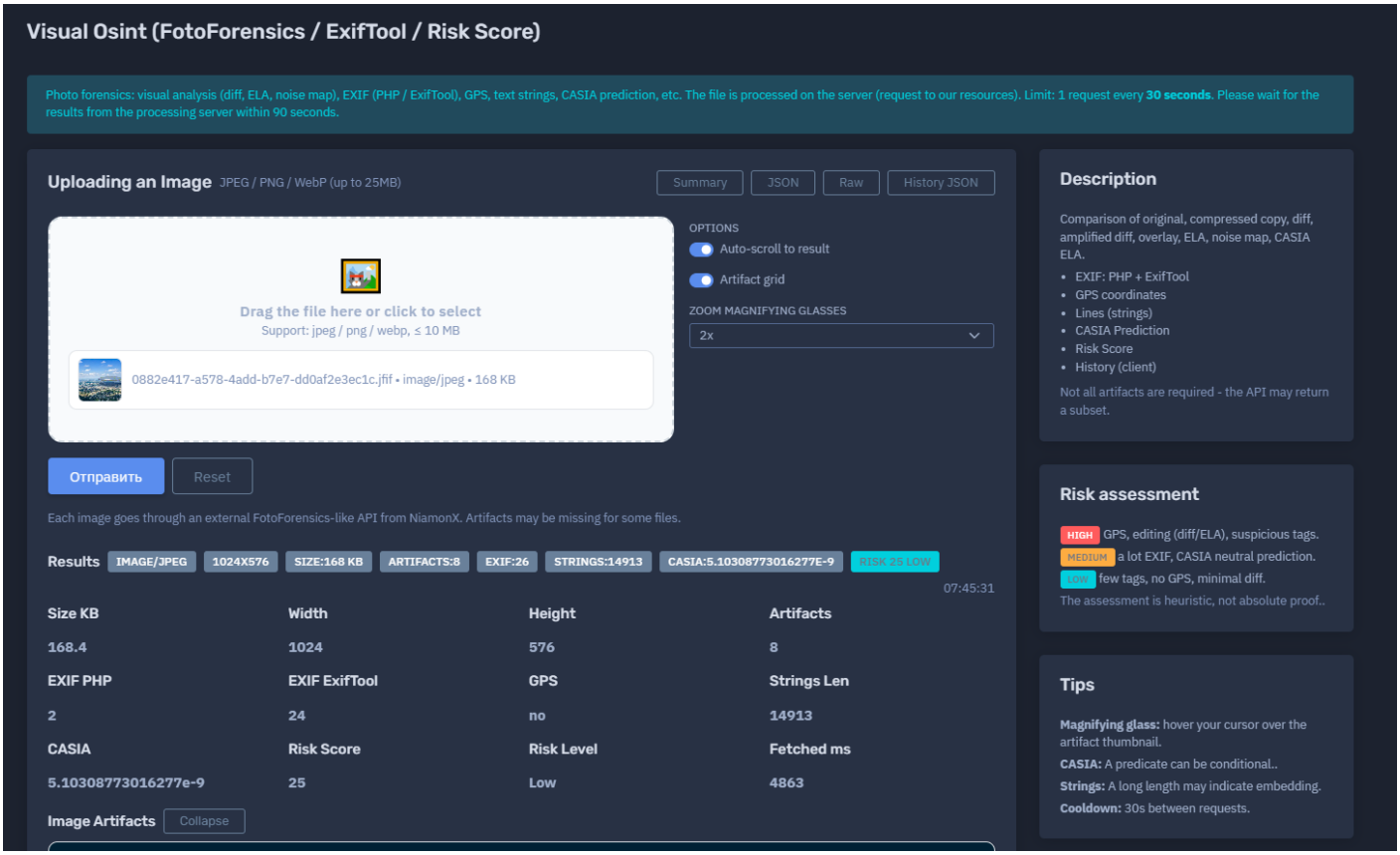
Each image receives a **heuristic Risk Score**, assessing the likelihood of manipulation or sensitive content presence:

- **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**.



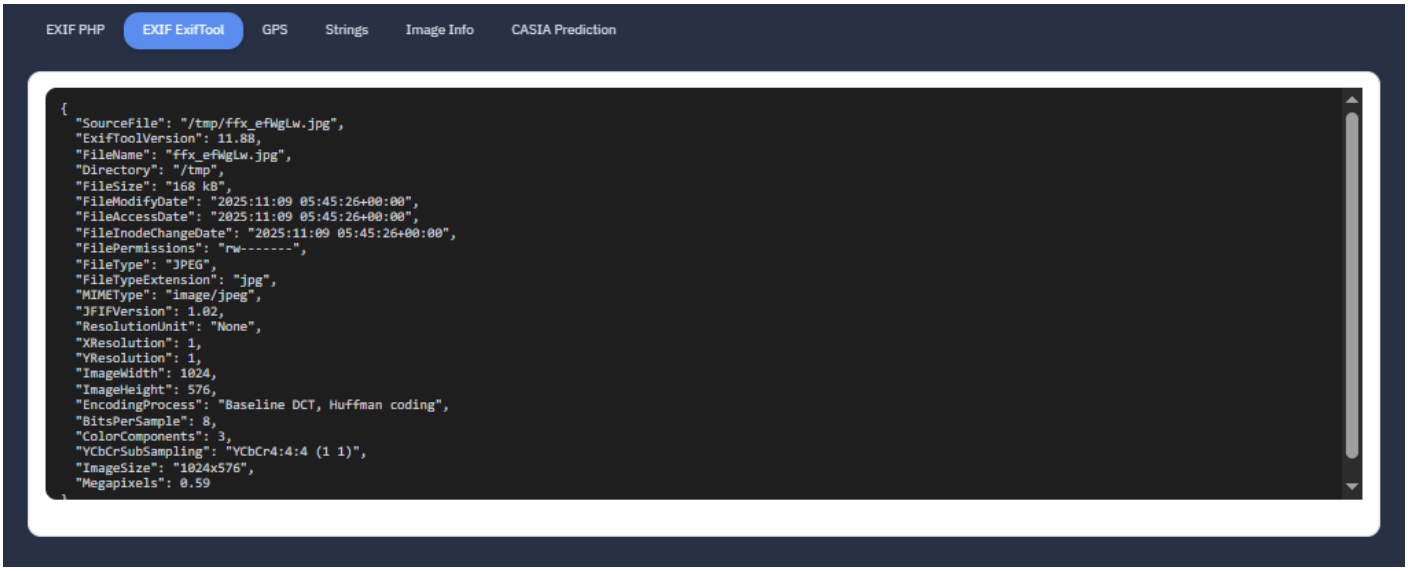
? Request History

- 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**.

Revision #1
Created 9 November 2025 05:46:43 by NiamonX Team
Updated 9 November 2025 05:52:09 by NiamonX Team