

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**.

Visual Osint (FotoForensics / ExifTool / Risk Score)

Photo forensics: visual analysis (diff, ELA, noise map), EXIF (PHP / ExifTool), GPS, text strings, CASIA prediction, etc. The file is processed on the server (request to our resources), Limit: 1 request every **30 seconds**. Please wait for the results from the processing server within 90 seconds.

Uploading an Image JPEG / PNG / WebP (up to 25MB)

Summary JSON Raw History JSON

Drag the file here or click to select
Support: jpeg / png / webp, ≤ 10 MB

0882e417-a578-4add-b7e7-dd0af2e3ec1c.jfif • image/jpeg • 168 KB

Отправить Reset

Each image goes through an external FotoForensics-like API from NiamonX. Artifacts may be missing for some files.

RESULTS IMAGE/JPEG 1024X576 SIZE:168 KB ARTIFACTS:8 EXIF:26 STRINGS:14913 CASIA:5.10308773016277E-9 RISK 25 LOW 07:45:31

Size KB	Width	Height	Artifacts
168.4	1024	576	8
EXIF PHP	EXIF ExifTool	GPS	Strings Len
2	24	no	14913
CASIA	Risk Score	Risk Level	Fetches ms
5.10308773016277e-9	25	Low	4863

Image Artifacts Collapse

Description

Comparison of original, compressed copy, diff, amplified diff, overlay, ELA, noise map, CASIA ELA.

- EXIF; PHP + ExifTool
- GPS coordinates
- Lines (strings)
- CASIA Prediction
- Risk Score
- History (client)

Not all artifacts are required - the API may return a subset.

Risk assessment

- HIGH** GPS, editing (diff/ELA), suspicious tags.
- MEDIUM** a lot EXIF, CASIA neutral prediction.
- LOW** few tags, no GPS, minimal diff.

The assessment is heuristic, not absolute proof..

Tips

Magnifying glass: hover your cursor over the artifact thumbnail.

CASIA: A predicate can be conditional..

Strings: A long length may indicate embedding.

Cooldown: 30s between requests.

? 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.

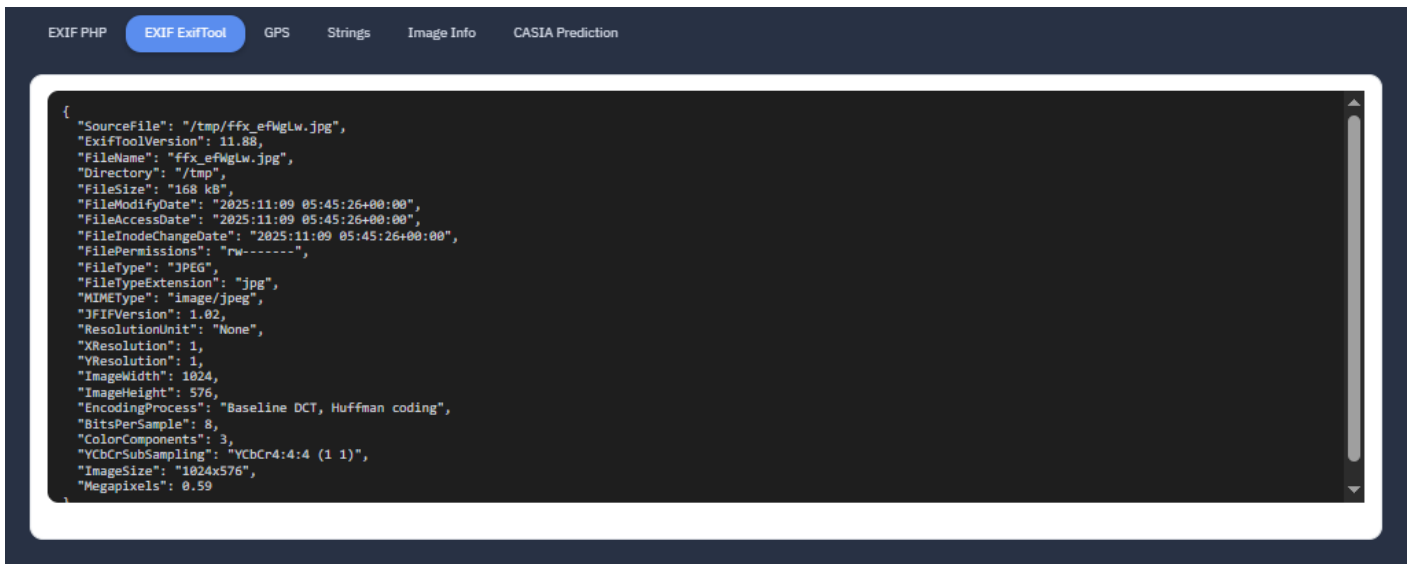
?? Security & Privacy

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.



```
{
  "SourceFile": "/tmp/ffx_efWgLw.jpg",
  "ExifToolVersion": 11.88,
  "FileName": "ffx_efWgLw.jpg",
  "Directory": "/tmp",
  "FileSize": "168 kB",
  "FileModifyDate": "2025:11:09 05:45:26+00:00",
  "FileAccessDate": "2025:11:09 05:45:26+00:00",
  "FileInodeChangeDate": "2025:11:09 05:45:26+00:00",
  "FilePermissions": "rw-----",
  "FileType": "JPEG",
  "FileTypeExtension": ".jpg",
  "MIMEType": "image/jpeg",
  "JFIFVersion": 1.02,
  "ResolutionUnit": "None",
  "XResolution": 1,
  "YResolution": 1,
  "ImageWidth": 1024,
  "ImageHeight": 576,
  "EncodingProcess": "Baseline DCT, Huffman coding",
  "BitsPerSample": 8,
  "ColorComponents": 3,
  "YCbCrSubSampling": "YCbCr4:4:4 (1 1)",
  "ImageSize": "1024x576",
  "Megapixels": 0.59
}
```

? Contact Information

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

- [support @ niamonx.io](mailto:support@niamonx.io) — Technical Support
- [other @ niamonx.io](mailto:other@niamonx.io) — General Questions
- [takedown @ niamonx.io](mailto:takedown@niamonx.io) — Requests for Data Removal / Privacy Takedowns
- [legal @ niamonx.io](mailto: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