TMA — True Media Analyzer

Digital Authenticity, Verified — Forensic Analysis for Images, Video & Documents

A Windows forensic desktop platform that examines images, video and documents for signs of digital tampering and forgery, delivering evidence-based verdicts built around proper case management.

15+
Forensic Engines

4-Tier
Evidence-Based Verdicts

Image+Video+Doc
Multi-Format Coverage

14-Day
Free Trial

Image Manipulation Detection

Detects copy-paste forgery, re-compression artifacts and duplicated or cloned regions within a photo, exposing edits invisible to the naked eye.

Fake Screenshot Detection

Identifies fabricated chat and SMS screenshots produced by online fake-chat generator tools, catching forged WhatsApp, Telegram and SMS evidence.

Document & Contract Forgery Detection

Flags PDFs and Word documents composited in image editors, tampered with after signing, or edited by someone other than the stated author.

Digital Signature Verification

Cryptographically validates PDF digital signatures to confirm a signed document has not been altered after signing.

Hidden Malware Detection

Scans documents for concealed malicious code, scripts and embedded executables hiding inside PDFs and Office files.

Video Forensics

Detects frame substitution, splicing, re-encoding and audio/video desync to determine whether a video has been edited or staged.

Evidence-Based Verdict Engine

Every file gets a clear, confidence-rated authenticity verdict instead of a raw score — built to withstand scrutiny in investigations and legal proceedings.

Case Management & Chain of Custody

Organises evidence into auditable cases with integrity verification, hash-based tamper checks and exportable case packages.

VERDICT CLASSIFICATION

CLEAN | INFORMATIONAL | SUSPICIOUS | LIKELY MANIPULATED

Built for digital forensics investigators, fraud examiners, legal/compliance teams and law enforcement.

info@cyber-zones.com