CYBERSHIELD INDIA

AI-Powered Cybercrime Forensic Analysis Report

AI-GENERATED CONTENT DETECTED

CASE INFORMATION

Case ID:	CASE-TEST-20260206-ABC123
Analysis Date:	2026-02-07T21:39:39.944747
Media Type:	IMAGE
Filename:	test_ai_image.jpg
File Hash (SHA-256):	a1b2c3d4e5f6g7h8i9j0k1l2m3n4o5p6...

DETECTION ANALYSIS

AI Detection Confidence:	87.00%
Detection Model:	Organika/sdxl-detector
Classification:	ARTIFICIAL
Risk Level:	HIGH - Strong AI signature

TECHNICAL FORENSIC ANALYSIS

Complete File Hash (SHA-256):

a1b2c3d4e5f6g7h8i9j0k1l2m3n4o5p6q7r8s9t0u1v2w3x4y5z6a1b2c3d4e5f6g7h8i9j0k1l2m3n4o5p6q7r8s9t0u1v2w3x4y5z6

Detection Breakdown:

Component	Score
ML Model Score	92.00%
Artifact Analysis	75.00%

BLOCKCHAIN EVIDENCE INTEGRITY

Status:	Pending
Transaction Hash:	Will be added in Step 5
Verification:	Evidence cryptographically secured

FORENSIC CONCLUSIONS

Based on comprehensive forensic analysis, this image exhibits strong indicators of artificial generation with 87.0% confidence. Multiple detection algorithms have identified patterns consistent with AI-generated content. The evidence suggests this media was created using generative AI technology rather than captured through traditional photography/videography methods. This finding is suitable for use in cybercrime investigations, legal proceedings, and platform moderation decisions.

DISCLAIMER

This report is generated using state-of-the-art AI detection algorithms and forensic analysis tools. While the system provides high-confidence assessments, no automated system is 100% accurate. This report should be used as supporting evidence in conjunction with other investigative methods. The blockchain timestamp provides cryptographic proof of when this analysis was conducted and that the evidence has not been tampered with since registration.

_____

Digital Forensic System Signature
Generated: 2026-02-07 21:39:39 UTC