CYBERSHIELD INDIA

AI-Powered Cybercrime Forensic Analysis Report

AI-GENERATED CONTENT DETECTED

CASE INFORMATION

Case ID:	CASE-20260208122616-a3b61e12
Analysis Date:	2026-02-08T06:56:22.730891
Media Type:	IMAGE
Filename:	Gemini_Generated_Image_2um5il2um5il2um5.jpg
File Hash (SHA-256):	afd97a0d57ebfdb5f5e552fcaa9198ac...

DETECTION ANALYSIS

AI Detection Confidence:	100.00%
Detection Model:	AI Detector
Classification:	ARTIFICIAL
Risk Level:	HIGH - Strong AI signature

MEDIA PREVIEW

TECHNICAL FORENSIC ANALYSIS

Complete File Hash (SHA-256):
`afd97a0d57ebfdb5f5e552fcaa9198ac936c219037712b18ad4db8691eb0cc35`

Detection Breakdown:

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 100.0% 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: 2026-02-08 12:26:22 UTC