

# CYBERSHIELD INDIA

AI-Powered Cybercrime Forensic Analysis Report

AI-GENERATED CONTENT DETECTED

## CASE INFORMATION

Case ID:	CASE-20260208123928-506311d4
Analysis Date:	2026-02-08T07:09:33.594504
Media Type:	IMAGE
Filename:	Gemini_Generated_Image_md40qbmd40qbmd40.jpg
File Hash (SHA-256):	cc088fd796e8fe2d6c5f32c5901d6fd4...

## DETECTION ANALYSIS

AI Detection Confidence:	99.50%
Detection Model:	AI Detector
Classification:	ARTIFICIAL
Risk Level:	HIGH - Strong AI signature

## MEDIA PREVIEW



## TECHNICAL FORENSIC ANALYSIS

**Complete File Hash (SHA-256):**

cc088fd796e8fe2d6c5f32c5901d6fd446a72eb7c3941253852e3e2b091c6fc

**Detection Breakdown:**

## BLOCKCHAIN EVIDENCE INTEGRITY

<b>Status:</b>	Pending blockchain registration
<b>Note:</b>	Will be anchored when gas is available

## FORENSIC CONCLUSIONS

Based on comprehensive forensic analysis, this image exhibits strong indicators of artificial generation with 99.5% 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 12:39:33 UTC