CYBERSHIELD INDIA

AI-Powered Cybercrime Forensic Analysis Report

AUTHENTIC CONTENT

CASE INFORMATION

Case ID:	CASE-20260207231506-de25287a
Analysis Date:	2026-02-07T17:45:06.782151
Media Type:	IMAGE
Filename:	real.jpg
File Hash (SHA-256):	e2a149b56d5f77c3a0f28bcaa499f8c4...

DETECTION ANALYSIS

AI Detection Confidence:	0.74%
Detection Model:	AI Detector
Classification:	AUTHENTIC
Risk Level:	LOW - Authentic content

MEDIA PREVIEW


Institute of Technology
Madras

TECHNICAL FORENSIC ANALYSIS

Complete File Hash (SHA-256):
`e2a149b56d5f77c3a0f28bcaa499f8c4a2d108987a8da6be8851344d996e1047`

Detection Breakdown:

BLOCKCHAIN EVIDENCE INTEGRITY

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

FORENSIC CONCLUSIONS

Forensic analysis suggests this image is likely authentic with a low AI-generation probability (0.7%). The content exhibits characteristics consistent with genuine capture methods. However, sophisticated AI techniques continue to evolve, and periodic re-evaluation may be warranted for high-stakes cases.

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 23:15:06 UTC