DIGITAL EVIDENCE ANALYSIS REPORT

REPORT IDENTIFICATION

Report ID:	EVD-8-20250917
Generated:	2025-09-17 14:23:12 UTC
Case ID:	8
Detection Type:	DEEPFAKE

CHAIN OF CUSTODY

Action: File Upload

Timestamp: 2025-09-17T08:53:04.158986

Details: Original file uploaded: 16bba215-e97b-46e0-90d7-aeac453fe86d_images.jpg

Action: Hash Calculation

Timestamp: 2025-09-17T08:53:04.158986

Details: SHA-256 hash calculated for integrity verification

Action: Analysis Performed

Timestamp: 2025-09-17T08:53:04.158986

Details: Deepfake detection analysis completed

Action: Evidence Report Generated

Timestamp: 2025-09-17T14:23:12.631336

Details: Court-ready evidence report created with digital signatures

TECHNICAL ANALYSIS RESULTS

Analysis Method:	CNN_classification
Model Version:	1.0

Prediction:	REAL
Confidence Level:	54.11%

LEGAL CERTIFICATION

I hereby certify that this analysis was conducted using scientifically accepted methods and industry-standard digital forensics practices.

The digital evidence was analyzed on September 17, 2025 using automated detection systems with a confidence level of 54.11%.

The integrity of the original digital evidence has been maintained throughout the analysis process, as verified by cryptographic hash validation.

This report contains the complete findings of the digital forensics analysis and has been generated automatically to ensure objectivity and reproducibility.

The methodologies employed are based on peer-reviewed research and are widely accepted in the digital forensics community.

All timestamps are recorded in UTC and can be independently verified through system logs.

INTEGRITY VERIFICATION

Original File Hash: b15285f38a62dcb8243b3439592bac1d191b4e819b88c84f939279c7b092ca01

Verification Status: VERIFIED

Verification Time: 2025-09-17T14:23:12.631336

METHODOLOGY

The deepfake detection analysis employs a convolutional neural network (CNN) trained on a large dataset of authentic and manipulated media.

The system analyzes facial features, temporal inconsistencies, and compression artifacts to identify potential manipulations.

For video files, multiple frames are sampled and analyzed independently, with results aggregated using statistical methods.

The confidence score represents the model's certainty in its prediction based on learned patterns from training data.