DIGITAL EVIDENCE ANALYSIS REPORT

REPORT IDENTIFICATION

Report ID:	EVD-1-20250916
Generated:	2025-09-16 16:32:14 UTC
Case ID:	1
Detection Type:	DEEPFAKE

CHAIN OF CUSTODY

Action: File Upload

Timestamp: 2025-09-16T10:47:05.690078

Details: Original file uploaded: 95cc9332-094a-4ad3-b373-3c6e49e731d6_WhatsApp_Image_2025-07-29_at_12.04.13_c701fe5c.jpg

Action: Hash Calculation

Timestamp: 2025-09-16T10:47:05.690078

Details: SHA-256 hash calculated for integrity verification

Action: Analysis Performed

Timestamp: 2025-09-16T10:47:05.690078

Details: Deepfake detection analysis completed

Action: Evidence Report Generated

Timestamp: 2025-09-16T16:32:14.878888

Details: Court-ready evidence report created with digital signatures

TECHNICAL ANALYSIS RESULTS

Analysis Method:	CNN_classification

Model Version:	1.0
Prediction:	FAKE
Confidence Level:	50.96%

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 16, 2025 using automated detection systems with a confidence level of 50.96%.

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: f16e9470e3f18839e39fe3ee667b873f02d0754b8a0be0fbb1b2d5acbe956da8

Verification Status: VERIFIED

Verification Time: 2025-09-16T16:32:14.883173

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.