

# DIGITAL EVIDENCE ANALYSIS REPORT

## REPORT IDENTIFICATION

Report ID:	EVD-3-20250916
Generated:	2025-09-16 16:27:25 UTC
Case ID:	3
Detection Type:	DEEPFAKE

## CHAIN OF CUSTODY

**Action:** File Upload

**Timestamp:** 2025-09-16T10:57:23.134799

**Details:** Original file uploaded: 4015b01f-5e0f-41d4-94cf-9a55ed1f8ef8\_WhatsApp\_Image\_2025-07-29\_at\_12.04.13\_c701fe5c.jpg

**Action:** Hash Calculation

**Timestamp:** 2025-09-16T10:57:23.134799

**Details:** SHA-256 hash calculated for integrity verification

**Action:** Analysis Performed

**Timestamp:** 2025-09-16T10:57:23.134799

**Details:** Deepfake detection analysis completed

**Action:** Evidence Report Generated

**Timestamp:** 2025-09-16T16:27:25.477920

**Details:** Court-ready evidence report created with digital signatures

## TECHNICAL ANALYSIS RESULTS

Analysis Method:	CNN_classification
------------------	--------------------

Model Version:	1.0
Prediction:	REAL
Confidence Level:	51.64%

## 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 51.64%.

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:** 2025-09-16T16:27:25.479051

## 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.