

REPORT ON IMAGE FILE



General Information

Report ID:

Date and Time: No Created Date and Time available in metadata

Investigation Case ID:

Analyst Name:

Organisation Name:

Input File Details

File Name: efbc7e7b-da50-43ef-8f67-848959affb19.jpg

File Type: JPG

File Size: 8.82 KB

Resolution:

Duration(for video):

Frame Rate(for video):

Deepfake Analysis Results

Confidence Score:

Deepfake Likelihood:

Suspicious Regions Identified:

Suspicious Frames(for video reports)

Number of suspicious frames:

Timestamps of suspicious frames:

Metadata and Forensic Details

File Metadata:

EXIF Data(for images):

Hash Value(SHA-256):9bbca3de921f70363ac7d30d83669fc87e70e5e157ae1ccc6741e9

Compression Artifacts:

Frame Manipulation Detection:

Observations and Expert Remarks

Summary of Findings:

Possible Manipulations Techniques:

Confidence Level:

Suggested Next Steps:

Conclusion and Signature

Final Verdict:

Forensic Analyst Signature and Stamp: