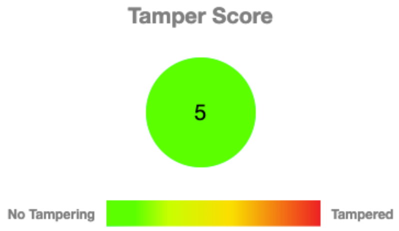
This report contains a summary of the analyzed JPEG files submitted to the Attestiv platform. Each image is evaluated using our 6-point forensic scan resulting in an aggregate tamper score.

Example:

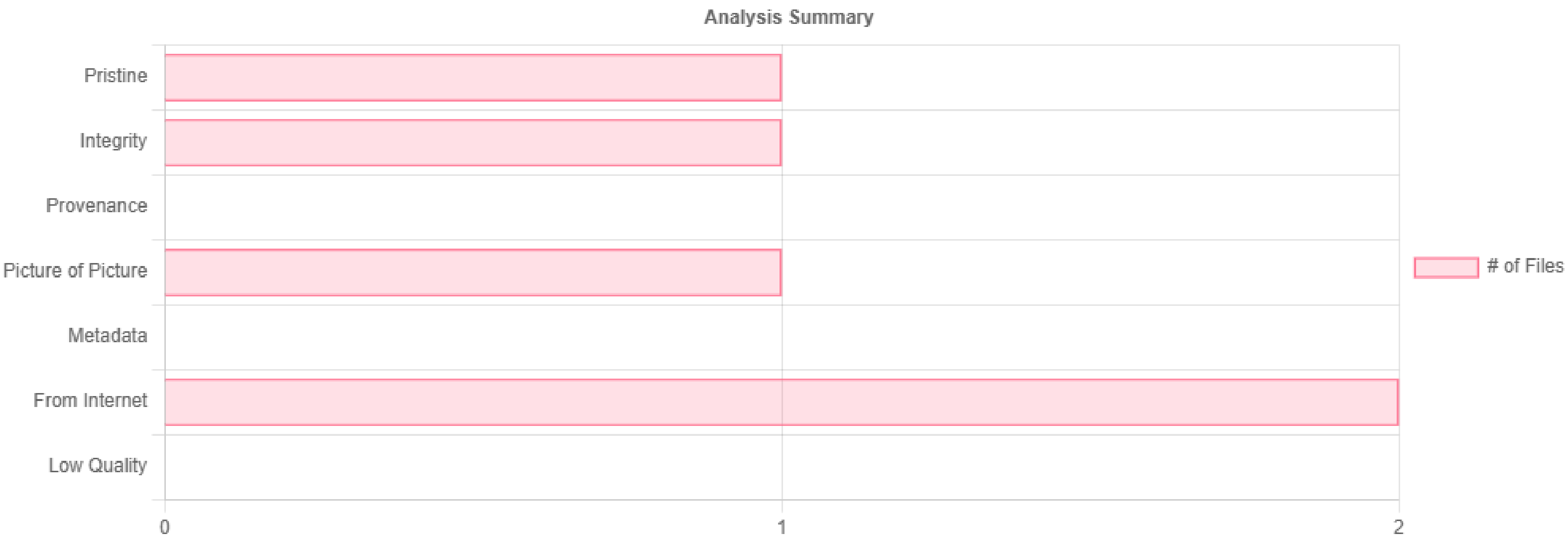


The 6 point scan includes metadata, provenance, photo of photo, image integrity, image quality, and a reverse search scoring. Definitions can be found in the table below.

Metadata Score
Provenance Score
Photo of Photo Score
Image Integrity Score
Image Quality Score
Reverse Search Score

The table below contains a summary of all the image files analyzed. Images with Tamper Scores with less than 50 are considered to be Pristine whereas for images with a Tamper Score greater than 50, the highest violating score will be displayed.

Analysis Method	Definition
Reverse Search Score	Assesses whether the image has been sourced from the internet.
Metadata Score	Assesses whether the image has traces of editing or other anomalies in the metadata.
Provenance Score	Assesses whether the image has forensic traces from known sources.
Image Integrity Score	Assesses whether the image file has any structural inconsistencies.
Image Quality Score	Assesses the level of blur and noise in the image. Attackers may use these defects to hide malicious edits.
Photo of Photo Score	Assesses whether the image is a photo of a photo.



Report Created By: Walid AL-SAQAF

Email: wsaqaf@gmail.com

Date: 10/28/2024

test2-f.png

Tamper Score

31

No Tampering **Tampered**

Metadata Score	🟩⬜⬜⬜⬜	
Provenance Score	🟩⬜⬜⬜⬜	
Photo of Photo Score	⬜⬜⬜⬜⬜	⚠
Image Integrity Score	🟩⬜⬜⬜⬜	
Image Quality Score	⬜⬜⬜⬜⬜	⚠
Reverse Search Score	🟨🟨⬜⬜⬜	⚠

⚠ Tamper Alerts

- Reverse Search: This image may have originated on the web.
- Quality: Analysis was skipped for this model because the size of the image was too small. The minimum image size required for this model to run is 640x480.
- Photo of Photo: Analysis was skipped for this model because the size of the image was too small. The minimum image size required for this model to run is 640x480.

test1-f.jpg

Tamper Score

100

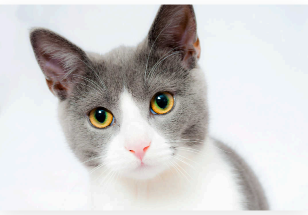
No Tampering **Tampered**

Metadata Score	🟩⬜⬜⬜⬜	
Provenance Score	🟥🟥🟥🟥🟥	⚠
Photo of Photo Score	🟩⬜⬜⬜⬜	
Image Integrity Score	🟧🟧🟧⬜⬜	
Image Quality Score	🟩⬜⬜⬜⬜	
Reverse Search Score	🟥🟥🟥🟥🟥	⚠

⚠ Tamper Alerts

- Provenance: This image has traces from a software package found in many editing tools.
- Reverse Search: This image may have originated on the web.

test4-r.jpg



Tamper Score

100

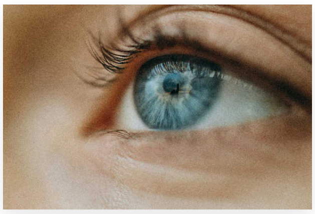
No Tampering **Tampered**

Metadata Score	🟥🟥🟥🟥🟥	⚠
Provenance Score	🟥🟥🟥🟥🟥	⚠
Photo of Photo Score	🟩⬜⬜⬜⬜	
Image Integrity Score	🟨🟨⬜⬜⬜	
Image Quality Score	🟩⬜⬜⬜⬜	
Reverse Search Score	🟥🟥🟥🟥🟥	⚠

⚠ Tamper Alerts

- Metadata: This image contains an unfamiliar ICC color profile. In general, cameras do not generate their own ICC Profiles.
- Provenance: This image has traces from a software package found in many editing tools.
- Reverse Search: This image may have originated on the web.

test3-r.jpg



Tamper Score

100

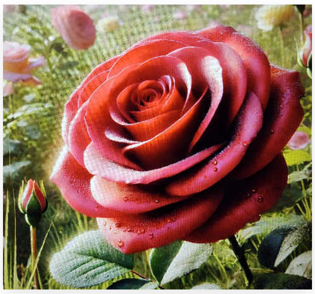
No Tampering — Tampered

Metadata Score	🟥🟥🟥🟥🟥	⚠
Provenance Score	🟥🟥🟥🟥🟥	⚠
Photo of Photo Score	🟧🟧🟧🟧⬜	⚠
Image Integrity Score	🟥🟥🟥🟥🟥	⚠
Image Quality Score	🟧🟧🟧🟧⬜	⚠
Reverse Search Score	🟥🟥🟥🟥🟥	⚠

⚠ Tamper Alerts

- Metadata: This image contains an unfamiliar ICC color profile. In general, cameras do not generate their own ICC Profiles.
- Provenance: This image has traces from a software package found in many editing tools.
- Quality: This image is very blurry or noisy.
- Reverse Search: This image may have originated on the web.
- Photo of Photo: This image appears to be a photo of a screen.
- Image Integrity: Generative AI probability: 0.93

test5-f.jpg



Tamper Score

100

No Tampering — Tampered

Metadata Score	🟥🟥🟥🟥🟥	⚠
Provenance Score	🟥🟥🟥🟥🟥	⚠
Photo of Photo Score	🟥🟥🟥🟥🟥	⚠
Image Integrity Score	🟩⬜⬜⬜⬜	
Image Quality Score	🟨🟨⬜⬜⬜	
Reverse Search Score	🟩⬜⬜⬜⬜	

⚠ Tamper Alerts

- Metadata: The media contains evidence of being edited by image editing software. The media has multiple dimensions defined in the metadata. It was likely scaled. The media contains evidence of being modified after it was captured.
- Provenance: This image has traces from a software package found in many editing tools.
- Photo of Photo: This image appears to be a photo of a screen.