Verifying images signed by Bill Toole

Images I publish may carry an invisible digital signature. It lets you check two things:

1. **Who signed it**: the image was signed with my private key.
2. **That it is unchanged**: no pixel has been altered since signing.

Verification happens entirely in your browser. Nothing is uploaded anywhere.

How to verify an image

1. Open sigstamp_verify.
2. Drag the signed **PNG** file onto the page, or click the box to choose it.
You can check several files at once.
3. Read the result:

Result	Meaning
Green: VALID	The image is exactly as signed. The author name and signing time are shown.
Red: INVALID	The image was modified after signing, or was signed with a different key.
Red: NO SIGNATURE	No signature was found. The image was never signed, or it was re-saved, resized, or compressed, which destroys the signature.

Confirm you are checking against my key

The verifier shows a **key fingerprint** under the drop area. Compare it with the one I have published. If the two match, the page is using my real key.

My key fingerprint (SHA-256):

shasum -a 256 79770ef9faab912b9dbe4b0c78cd1b27a1eabf31b1138e5924a507f41d5d2e68

I also publish this fingerprint here.

Matching the first 12 to 16 characters is enough for a quick check. If the fingerprints differ, do not trust the result.

Important: get the original file

The signature lives in the pixel data itself, so anything that re-encodes the image removes it. These will **not** verify:

- Screenshots or photos of the image
- Images sent through messaging apps, social media, or email previews that compress or resize them
- Files converted to JPEG or another format, cropped, resized, or edited

Ask for the original PNG file (a download link or a zip works best).
Only 8-bit RGB PNG files are supported.

What a green result does and does not prove

It proves that the pixels are identical to what was signed, and that whoever signed it holds the private key matching the fingerprint above.

It does not prove that the image is a true depiction of events, or that the signing time is exact. The time comes from the signer's own computer clock. Who the key belongs to depends on the fingerprint check above.

Browser support

The verifier needs a browser with Ed25519 support: Firefox 129 or newer, Chrome 137 or newer, or Safari 17 or newer. Older browsers will show a message saying so.

Questions

Email me.