1. EXIF METADATA & C2PA CONTENT CREDENTIALS ANALYSIS TOOL: EXIFTOOL / CONTENTAUTHENTICITY.ORG

1 CLI Metadata Extraction via Phil Harvey's ExifTool

Execute these commands in Terminal (macOS/Linux) or PowerShell (Windows) to audit camera hard-coded metadata vs. software modification tags.

```
# 1. Extract all software, camera hardware, and GPS metadata tags
exiftool -a -u -g1 supplier_factory_photo.jpg

# 2. Audit specifically for AI generation, Photoshop, or canvas alterations
exiftool -Software -CreatorTool -HistorySoftwareAgent -ApplicationNotes supplier_factory_photo.jpg

# 3. Verify original capture timestamp against file modification date
exiftool -DateTimeOriginal -CreateDate -ModifyDate -FileModifyDate supplier_factory_photo.jpg
```

Exif Metadata Tag	Authentic Camera Indicator	AI / Photoshop Manipulation Red Flag
Software / CreatorTool	Camera Firmware (e.g., *Canon EOS R5 v1.8.0*)	`Adobe Photoshop 25.0`, `Midjourney`, `Stable Diffusion`, `DALL-E`
Bits Per Sample / Color Space	Standard sRGB / Adobe RGB raw sensor profiles	Missing profiles, web-optimized stripped metadata (0 bytes EXIF block)
C2PA Manifest (CR)	Valid cryptographic signature chain from hardware sensor	Manifest flag: `"actions": ["c2pa.edited", "generative_fill"]`

2 C2PA Content Credentials Web Verification

Drag and drop images into **Verify.contentauthenticity.org** or **ContentCredentials.org/verify**. If the media was produced or edited using Generative AI engines (Photoshop Generative Fill, Firefly, Midjourney v6+), the C2PA parser will output a explicit "Content Credentials" tree revealing the base visual prompts and tool history.

2. ERROR LEVEL ANALYSIS (ELA) & COMPRESSION NOISE AUDIT TOOL: FOTOFORENSICS / FORENSICALLY

ELA highlights differences in JPEG compression error levels across an image. Re-saved or digitally inpainted regions (such as fake logos on machines or altered certificate text) degrade at different rates than the surrounding background.

3 How to Read ELA Diagnostics on FotoForensics.com

- **Uniform Brightness / White Noise:** Uniform high-frequency edges (normal for high-contrast real surfaces).
- **Asymmetrical Bright Highlights:** If a logo, text box, or serial number plate glows significantly brighter than surrounding textures of identical material, that specific region was digitally inserted or edited recently.
- **Solid Dark Regions:** Represents flat surfaces or areas that have been saved repeatedly without modification.

> **CRITICAL ELA RULE:** Do not analyze low-resolution WhatsApp or WeChat screenshots. Social messaging apps re-compress images completely, erasing forensic ELA traces. Always demand the **uncompressed original file (PNG or raw JPEG file attachment)** directly from the supplier.

3. CERTIFICATE QR CODE & DOMAIN VERIFICATION PROTOCOL — TARGET: ISO / SGS / TÜV / CE FRAUDULENT CERTIFICATES

Fraudulent suppliers often print legitimate-looking QR codes on fake certificates that redirect buyers to lookalike verification sites controlled by the fraudster rather than the official registrar.

4 Step-by-Step Certificate QR Audit Workflow

1. **Scan with Raw Barcode Reader:** Use a raw QR reader app (not standard camera auto-open) to extract the plain destination URL without launching the browser immediately.
2. **Domain Root Inspection:** Verify the root domain against the official registrar list below. Beware of typo-squatted domains (e.g., `sgs-verify-cert.com` instead of `sgs.com`).
3. **WHOIS & Domain Age Check:** Run a `whois` search on the target domain. If the certification lookup domain was registered recently (e.g., less than 1 year ago) via anonymous proxy, it is a phishing portal.

Issuing Agency	Official Legitimate Verification Portal	Known Spoofing Pattern / Phishing Trap
SGS Certification	`sgs.com/en/verify-certification`	`sgs-verification-check.net`, `sgs-cert.org`
TÜV Rheinland	`certipedia.com` (Official TÜV database)	`tuv-certipedia-verify.com`, `tuv-approved.cn`
ISO Compliance	`iafcertsearch.org` (Official IAF Database)	Direct supplier-hosted verification landing pages
Bureau Veritas	`bureauveritas.com/service-desk`	`bv-verification-portal.com`

RED FLAG ALERT: If scanning a certificate QR code prompts for login credentials, asks to download an APK/executable file, or uses HTTP (instead of secure HTTPS), immediately flag the supplier as HIGH-RISK FRAUD.