Metadata Viewer Guide for Untraceable Creators

They don’t need the file. They just need the metadata.

Why This Matters

Your documents, photos, and exported PDFs are snitching.

Before a client opens your file, before you publish that blog post, even before you click "send" there is already a **trail of timestamps, locations, devices, usernames, and hidden data** stitched into the file itself.

That’s metadata. And it’s leaking without your permission.

Surveillance doesn’t need access to your *content*. It just needs context:

- Who created it
- Where and when
- What software
- What system name
- What GPS location
- What email or username is embedded

Most creators never check. That’s a mistake.

What to Do

Below is your minimalist, cross-platform guide to **viewing, stripping, and understanding metadata** like a ghost.

Step 1: View Metadata (Pick Your Tool)

1. exiftool (Advanced, Full Control)

Works on: macOS, Linux, Windows
Install:

```
brew install exiftool        # macOS
sudo apt install libimage-exiftool-perl  # Debian/Ubuntu
```

Use:

```
exiftool yourfile.jpg
exiftool yourfile.pdf
```

What it shows:
Every hidden tag embedded in your file: date created, GPS data, author name, camera serial, software versions, and more.

2. MAT2 (Metadata Anonymization Toolkit)

Works on: Linux (best), macOS via Homebrew
Install:

```
sudo apt install mat2
```

Use to inspect:

```
mat2 yourfile.png --show
```

Use to clean:

```
mat2 yourfile.png
```

Bonus:

Supports Office files, PDFs, JPGs, PNGs, and more. Outputs cleaned files with .clean appended.

Step 2: Understand What You're Seeing

Here's what to look for (and strip):

Field	Risk	Example
Author	Exposes your real name or OS login	"JSmith"
Creator Tool	Shows what software you used	Microsoft Word 2019
GPSLatitude/Longitude	Physical location of where file was created	37.7749 N, 122.4194 W
Create Date / Modify Date	Timestamps of activity	2025-06-30 10:43:12
Camera Serial / Make	Identifies device used	Canon EOS 5D Mark III

Step 3: Strip It Clean

You've got two safe, local ways to nuke the metadata:

1. With exiftool:

```
exiftool -all= yourfile.jpg
```

Creates a clean version and backs up the original.

2. With mat2:

```
mat2 yourfile.pdf
```

No metadata. No slip ups.

EXTRA THIRD OPTION:

3. qpdf (Strip Hidden PDF Metadata)

Works on: Linux, macOS, Windows
Use it when: MAT2 doesn't fully clean PDFs or metadata lingers from LibreOffice, Microsoft Word, or other editors.

Install:

```
sudo apt install qpdf       # Debian/Ubuntu
brew install qpdf           # macOS
```

View basic info:

```
qpdf --show-encryption Metadata-Viewer.pdf
```

Clean it:

```
qpdf --linearize --object-streams=disable --remove-unreferenced-resources Metadata-Viewer.pdf Cleaned.pdf
```

note:

--linearize: Optimizes for fast web viewing (optional but helpful)

--object-streams=disable: Avoids preserving old structures

--remove-unreferenced-resources: Cuts leftover embedded junk

Then verify cleanup:

```
mat2 Cleaned.pdf --show
```

If fields like creator, producer, or mod-date are gone or null, you're good.

Final Note

You can encrypt your vault. Use Tuta. Use Signal. But if your files carry your fingerprint, you're still bleeding data.

Before you publish, share, or send **check what they see.** *Because that one file might tell more of your story than you think.*

Create. Encrypt. Control it all

https://untraceabledigitaldissident.com