Dangerzone

your documents

FOSDEM 2026

Alex Pyrgiotis (@apyrgio)
Freedom of the Press Foundation

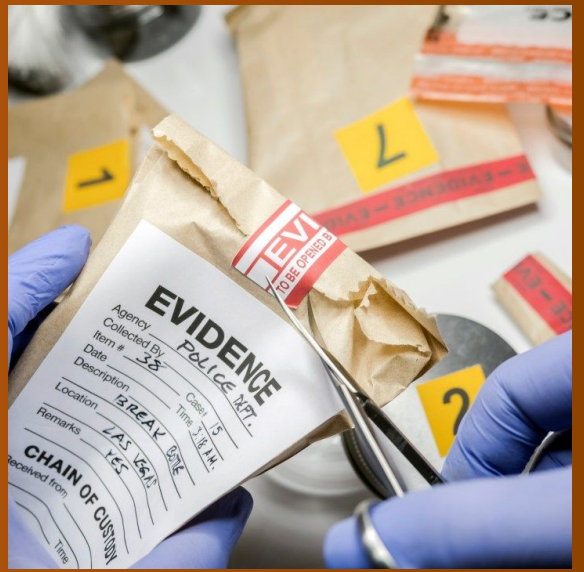
What is this talk about?

- Examples of known de-anonymization vectors
- Tools that can help you anonymize your documents
  - ... and their limitations
- Dampening the technical and psychosocial effects of these limitations

What is this talk NOT about?

- A novel approach to remove sophisticated traitor tracing schemes
- A technical deep dive on metadata removal
- A comparison of current tools to find out “the best”
- Advice on how to anonymously obtain and share sensitive documents
    - But use Tails though

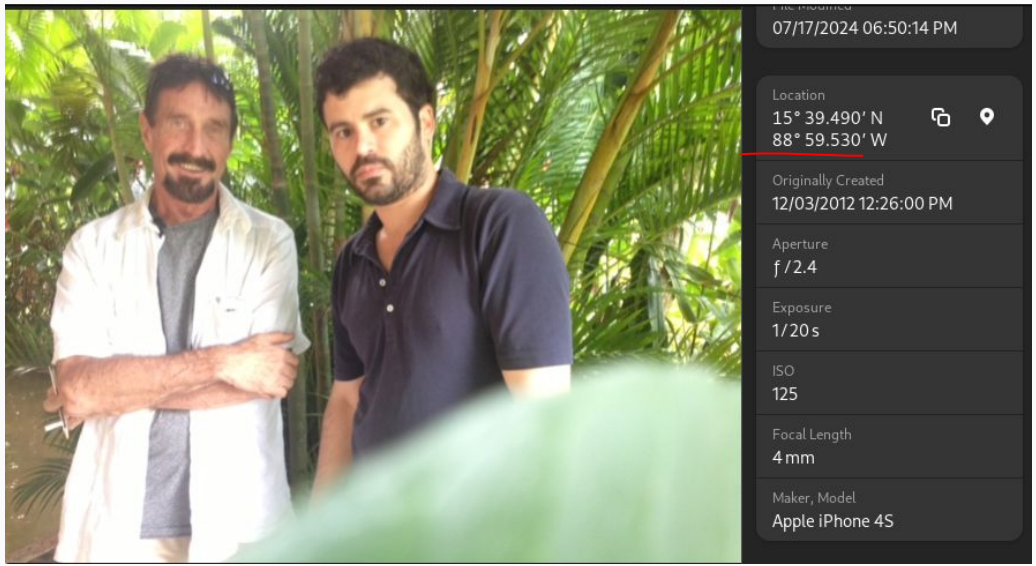
De-anonymization vectors



De-anonymization vectors

- Lots of historical examples of de-anonymization from files
  - We won't talk about OPSEC failures
- Possibly unknown terms:
  - OCR: Optical Character Recognition
  - Flatten: Squash all components of a page into an image
- Metadata are just the tip of the iceberg
- We tried to categorize all known examples
  - If you have an example that doesn't fall in one of those categories, **speak up!**

Exhibit A - Simple metadata (photos, audio, video)



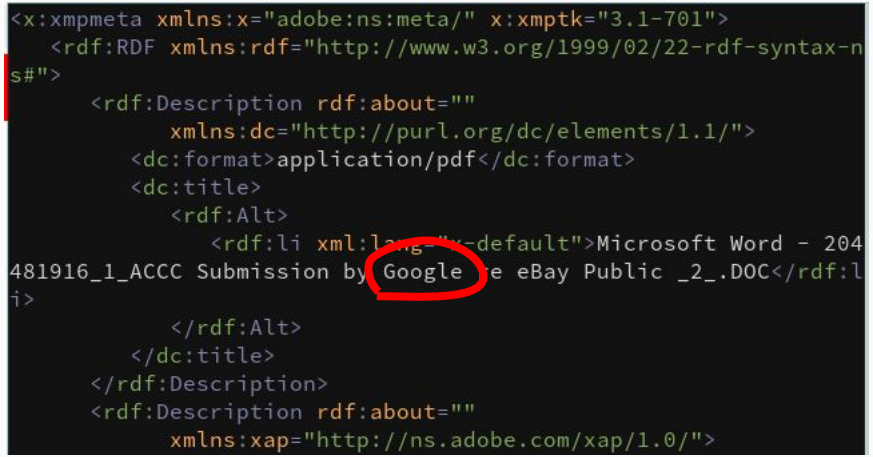
WIRED

Oops! Did Vice Just Give Away John McAfee's Location With Photo Metadata?

https://www.wired.com/2012/12/oops-did-vice-just-give-away-john-mcafees-location-with-this-photo/

⚠️Photos may contain location and author info
💡Scrub the metadata before sharing

Exhibit B - Complex metadata (PDF, office documents)



The Register

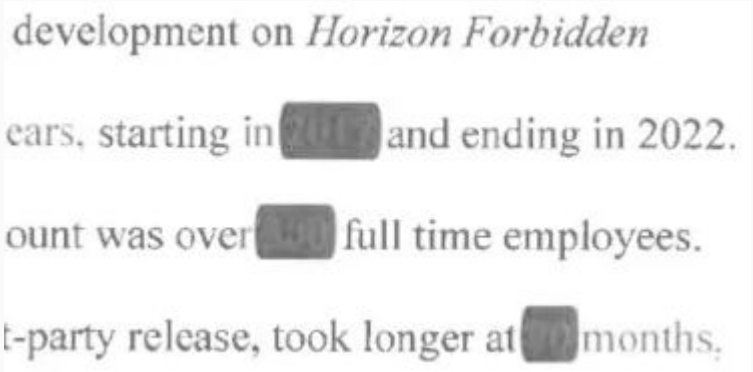
Metadata ruins Google's anonymous eBay Australia protest

https://www.theregister.com/2008/05/30/metadata_ruins_google_accc_filing/

⚠️ PDFs and office documents may contain **nested** metadata.
Think embedded photos, Word's tracking changes feature.

💡 Flatten the document to remove them

Exhibit C - Redactions


development on *Horizon Forbidden*

ears, starting in [redacted] and ending in 2022.

ount was over [redacted] full time employees.

t-party release, took longer at [redacted] months.

The Verge

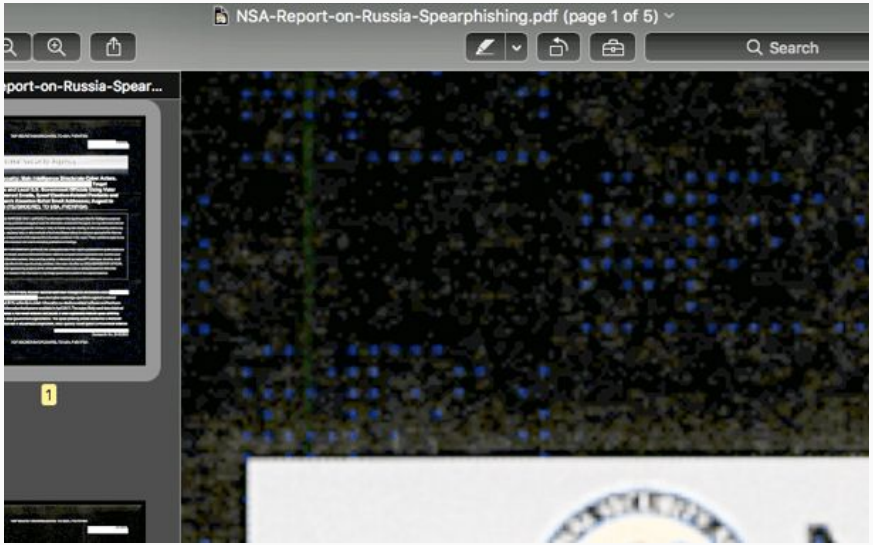
Sony's confidential PlayStation secrets just spilled because of a Sharpie / The black Sharpie strikes again to reveal Sony's Call of Duty revenue secrets.

https://www.theverge.com/2023/6/28/23777298/sony-ftc-microsoft-confidential-documents-marker-pen-scanner-oops

⚠️ Redactions do not work if in a layer or not opaque

💡 Use opaque black bars and then flatten the document

Exhibit D - Physical watermarks



The Atlantic

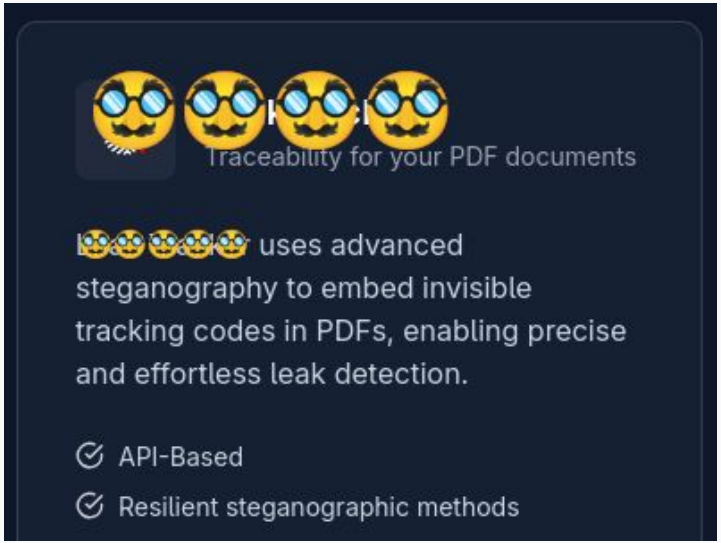
The Mysterious Printer Code That Could Have Led the FBI to Reality Winner

Many color printers embed grids of dots that allow law enforcement to track every document they output.

https://www.theatlantic.com/technology/archive/2017/06/the-mysterious-printer-code-that-could-have-led-the-fbi-to-reality-winner/529350/

⚠️ Printed documents may contain tracking dots
💡 OCR the document and copy the text to a new one

Exhibit E - Digital watermarks

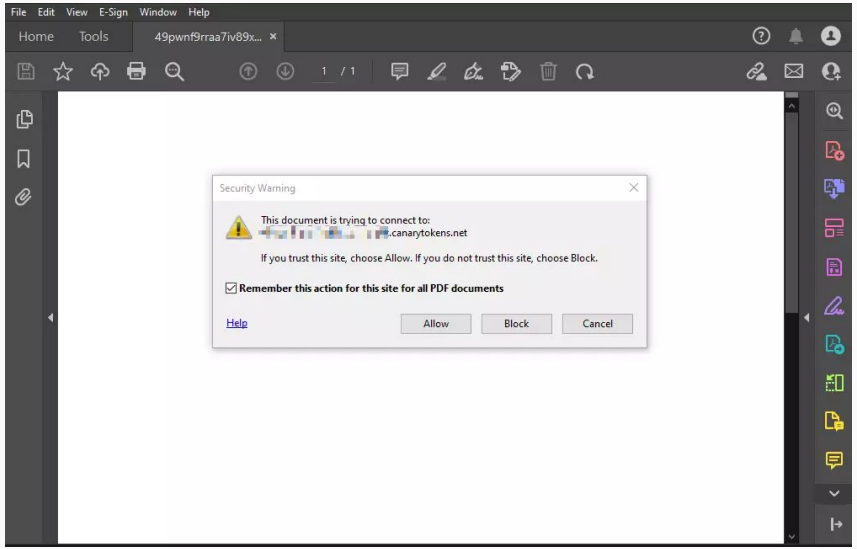


⚠️ Digital material accessible only to you may have invisible watermarks
💡 OCR the document, double translate (e.g., English -> Chinese -> English)

Exhibit E - Digital watermarks

No way to be 100% safe

Exhibit F - Canary tokens

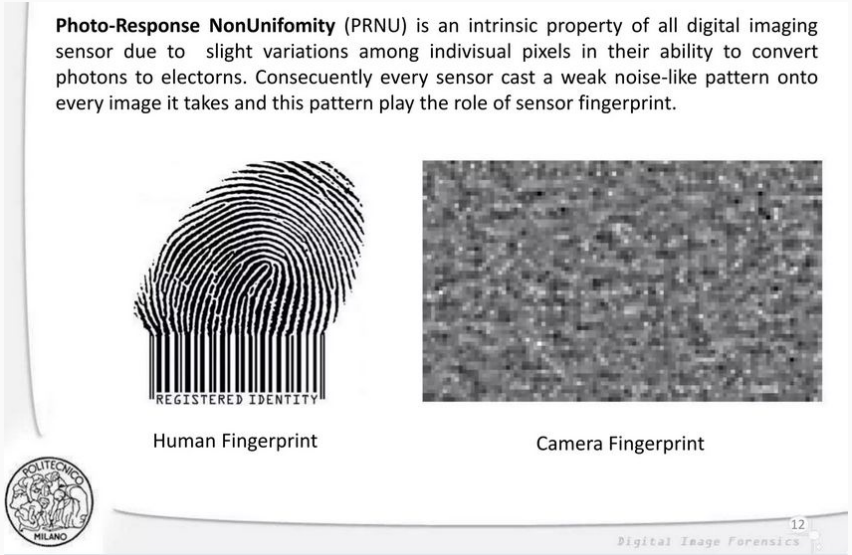


- Most sane document viewers block them silently
- Microsoft Office ask to enable macros
- Adobe Acrobat asks if it's ok to connect
- Deanonymization is a click away

https://canarytokens.org/nest/
https://blog.amartinsec.com/blog/canary/

⚠️ Trapped documents may phone home in major viewers
💡 Flatten the document to remove them

Exhibit G - Fingerprinting



- Cameras, mics are subject to fingerprinting
- Your way of writing is a fingerprint (stylometry)
- Unlike watermarking, fingerprinting is useful only with a second match (much like human fingerprints)

Digital Image Forensics
Camera Fingerprint and its Robustness
https://www.slideshare.net/slideshow/digital-image-forensics-camera-fingerprint-and-its-robustness/15069696

⚠️ A/V equipment and writing style can be fingerprinted
💡 (A/V) Use disposable equipment
(writing) use common words, double translate

Exhibit G - Fingerprinting

No way to be 100% safe

Exhibit H - Environment

Japanese “Sasaeng” Tracked down a Female Idol’s Home by Zooming in on the Reflection in Her Eyes

https://www.koreaboo.com/stories/matsuoka-ena-sasaeng-obsessed-fan-idol-stalker-photo-eyes-reflection/

⚠️ Cameras, microphones capture the surrounding environment
💡 Avoid reflective surfaces and locations that can be associated with you

Exhibit H - Environment

No way to be 100% safe

Existing Tools

Exiftool

- De-facto tool to view and remove image metadata
- Supports other file types as well
- Retains the same filetype, snips only the meta
- Predominantly CLI, but has a GUI version as well

https://exiftool.org/

Reads .pdf metadata as well!

```
$ exiftool ~/Downloads/test.pdf
[...]
Producer                        : iText® 5.5.10 ©2000-2015 iText Group NV
(AGPL-version); modified using iText® 5.5.10 ©2000-2015 iText Group NV (AGPL-version)
Create Date                     : 2024:03:29 10:53:50+02:00
Modify Date                     : 2024:03:29 10:53:50+02:00
```

Looks like it can alter them...

```
$ exiftool -all:all= ~/Downloads/test.pdf
Warning: [minor] ExifTool PDF edits are reversible. Deleted tags may be recovered! -
/home/apyrgio/Downloads/test.pdf
    1 image files updated

$ exiftool ~/Downloads/test.pdf
[...]
```

But wait, what's this warning?

Exiftool

```
$ vimdiff ~/Downloads/test.pdf ~/Downloads/test-bak.pdf
```

Exiftool

File Type	Support	Description	EXIF	IPTC	XMP	ICC[1]	C2PA
PDB, PRC	R	Palm Database	-	-	-	-	-
PDF	R/W[7]	Adobe Portable Document Format	R[3]	R[3]	R/W/C	R[3]	R

Writer Limitations

- ExifTool will **not rewrite a file if it detects a significant problem** with the file format.
- ExifTool has been tested with a wide range of different images, but since it is not possible to tes
  possibility that it will corrupt some files. Be sure to keep backups of your files.
- Even though ExifTool does some validation of the information written, it is still **possible to write**
  when reading the images with other software. So take care to validate the information you are w
- ExifTool is **not guaranteed to remove metadata completely** from a file when attempting to de
  segments (except Adobe APP14, which is not removed by default) and trailers are removed whi
  other formats the results are less complete:
  - JPEG - APP segments (except Adobe APP14) and trailers are removed.
  - TIFF - XMP, IPTC, ICC_Profile and the ExifIFD are removed, but some EXIF may remain
    provided to simplify removal of common metadata tags from IFD0.)
  - PNG - Only XMP, EXIF, ICC_Profile and native PNG textual data chunks are removed.
  - PDF - The original metadata is never actually removed.
  - PS - Only XMP and some native PostScript tags may be deleted.
  - MOV/MP4 - Most top-level metadata is removed.
  - RAW formats - It is not recommended to remove all metadata from RAW images because
    information that is necessary for proper rendering of the image.

Turns out Exiftool appends its own metadata to the document, but doesn't remove the existing ones.

MAT2

- Supports lots of file types (video, audio, PDFs, office documents)
- Very thoughtful threat model
- Flattens some file types (PDFs, SVGs), removes metadata in others
- GUI option exists (Metadata Cleaner) but it’s not maintained
- Web option exists as well (mat2-web)
- Isomorphic sanitization, i.e., you get back the same filetype

https://github.com/jvoisin/mat2

MAT2

```
# Show potentially identifiable metadata in a document
$ mat2 -s ~/Downloads/tails_practical.docx
[+] Metadata for /home/apyrgio/Downloads/tails_practical.docx:
[++] Metadata for [Content_Types].xml:
      create_system: Weird
      date_time: 2024-01-15 15:13:40
[...]

# Clean potentially identifiable metadata from a document
$ mat2 ~/Downloads/tails_practical.docx

# Check there are none left
$ mat2 -s ~/Downloads/tails_practical.cleaned.docx
  No metadata found in /home/apyrgio/Downloads/tails_practical.cleaned.docx.
```

“While mat2 is doing its very best [...] there is no reliable way to detect every single possible metadata for complex file formats. This is why you shouldn't rely on metadata's presence to decide if your file must be cleaned or not.”

– *https://github.com/jvoisin/mat2?tab=readme-ov-file#notes-about-detecting-metadata*

Dangerzone

- Supports lots of document types, but not audio and video
- Mainly used to sanitize malware, removing metadata is a side-effect
- Based on Qubes' TrustedPDF
- Available on Windows, macOS, aimed at less experienced users
- Flattens every file, i.e., you get back just a PDF
- Maintained by Freedom of the Press Foundation (disclaimer: I work on this)

https://dangerzone.rocks/

```
# Sanitize a document
$ dangerzone-cli ~/Downloads/tails_practical.docx --ocr-lang eng
Assigning ID '2OMWo-' to doc '/home/apyrgio/Downloads/tails_practical.docx'
[...]
[doc 2OMWo-] 0% Converting page 1/8 from pixels to searchable PDF
[doc 2OMWo-] 12% Converting page 2/8 from pixels to searchable PDF
[doc 2OMWo-] 25% Converting page 3/8 from pixels to searchable PDF
[...]
Safe PDF(s) created successfully
/home/apyrgio/Downloads/tails_practical-safe.pdf
```

Tool summary

- Metadata removal is faster than flattening, and keeps file editable
- Flattening removes more de-anonymization vectors though
- Whistleblowers may not be technical, so tools must be misuse-resistant
- Compared to Dangerzone, MAT2 produces editable files, it's faster and supports more file types
- On the other hand, Dangerzone makes no assumptions about the document and is better at sanitizing everything

Tool summary

	Simple metadata	Complex metadata	Redactions	Physical watermarks	Digital watermarks	Canary tokens	Fingerprinting	Environment
Exiftool	✅	❌	❌	❌	❌	❌	❌	❌
MAT2	✅	⚠️	❌[1]	❌	❌	❌	❌	❌
Dangerzone	✅	✅	⚠️	⚠️[2]	❌	✅	❌	❌

[1] Not all file types can be redacted
[2] Assumes use of OCR feature

What is to be done?

What is to be done?

- Tools like Dangerzone are a good first step
- Some vectors can be removed, but the file will seem forged
- Others cannot be removed at all
- What should happen when anti-forensics projects can’t offer a technical solution?

When an action is unsafe but people will do it anyway...

... we should at least offer them clear and easy to follow advice

Harm reduction

- The rest of the presentation is about practical advice to sources and whistleblowers
- Centered around Dangerzone, but applies to other tools that flatten documents
- Main goal is to avoid common mistakes
  - Again, we are strictly speaking about file contents
  - **Speak up** if you know of another good protection

Harm reduction – Audio and video

Not supported by Dangerzone, use MAT2. Also:

1. **Did you record it?** Use disposable equipment and locations away from you
2. **Accessible only by you or a group?** Ask not to go public
3. **Always remember:** No 100% safe way to anonymize

Vectors: Simple metadata, digital watermarks, fingerprinting, environment

Harm reduction - Images

Sanitize with Dangerzone after obtaining and before sharing. Also:

1. **Did you capture it?** Use disposable equipment and locations away from you
2. **Accessible only by you or a group?** Ask not to go public
3. **Did you print it or scan it?** Original files, else ask not go public
4. **Redactions:** Edit with black opaque bars
5. **Always remember:** No 100% safe way to anonymize

Vectors: Simple metadata, redactions, physical watermarks, digital watermarks, fingerprinting, environment

Harm reduction - Documents

Sanitize with Dangerzone after obtaining and before sharing. Also:

1. **Did you print it?** OCR it or retype it
2. **Redactions:** Edit with black opaque bars
3. **Accessible only by you or a group?** OCR it or retype it, and then double translate it. In any case, prefer not to go public.
4. **Did you write it?** Change tone of writing, use common words, double translate. In any case, prefer not to go public.
5. **Always remember:** No 100% safe way to anonymize

Vectors: Simple/complex metadata, redactions, physical watermarks, digital watermarks, fingerprinting

tl;dw

- Anonymity means more than removing metadata
- No technical solution against all tracing methods
- Tools must be misuse-resistant and part of harm reduction logic

Get involved!

Issues and PRs super welcome:
🐙 freedomofpress/dangerzone

Dust off your RSS reader:
🌐 https://dangerzone.rocks/news

Ixnay on the algorithm:
🐘 social.freedom.press/@dangerzone