INTRODUCTION TO CONTENT CREDENTIALS

LEONARD ROSENTHOL

ADOBE, CONTENT AUTHENTICITY ARCHITECT
C2PA, CHAIR TECHNICAL WORKING GROUP

PROVENANCE (/ˈPRɒV(ə)NəNS/):
"THE BEGINNING OF SOMETHING'S EXISTENCE; SOMETHING'S ORIGIN"…

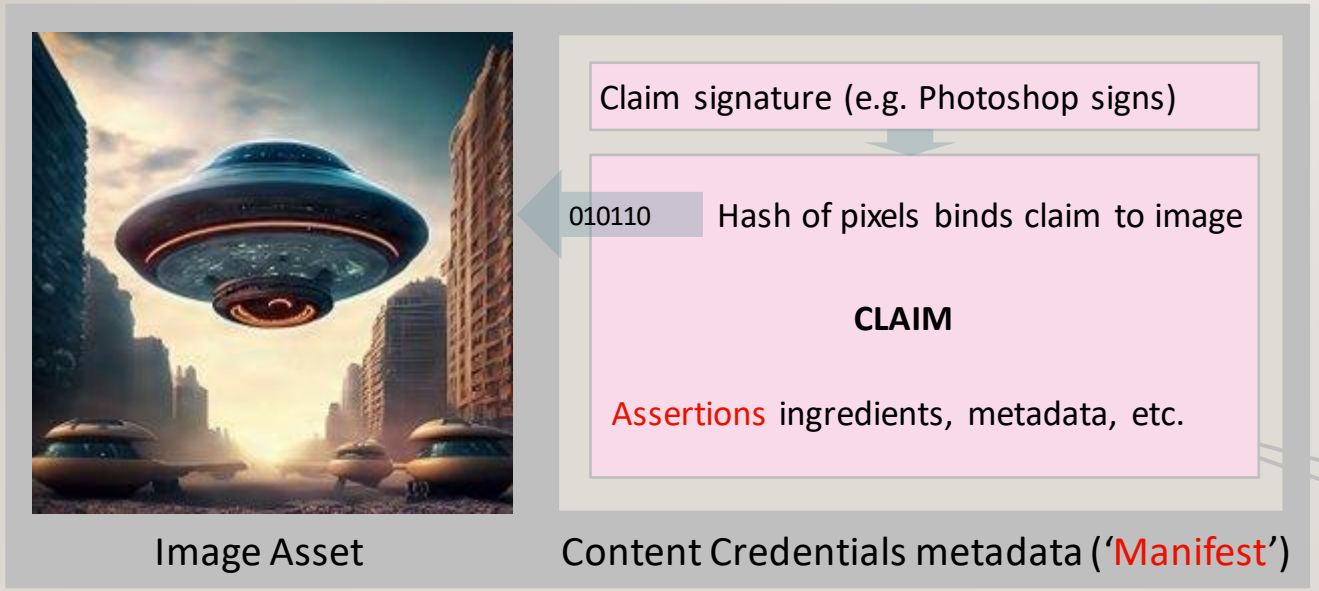
- It's not an arms race
- Edits are good!

Instead of guessing what is fake, we can provide information about the truth.

C2PA: COALITION FOR CONTENT PROVENANCE AND AUTHENTICITY

Content Credentials establish content provenance and authenticity at scale to give publishers, creators, and consumers the ability to trace the origin of media.

C2PA is a Linux Foundation Joint Development Foundation project specifying provenance metadata



C2PA Manifest contains signed claim

Claim contain facts called assertions

Assertions describe how an asset was made, by who, using what etc.

Can link to manifests in ingredient assets to form a provenance graph

content credentials

C2PA MEMBERSHIP AND ADOPTION

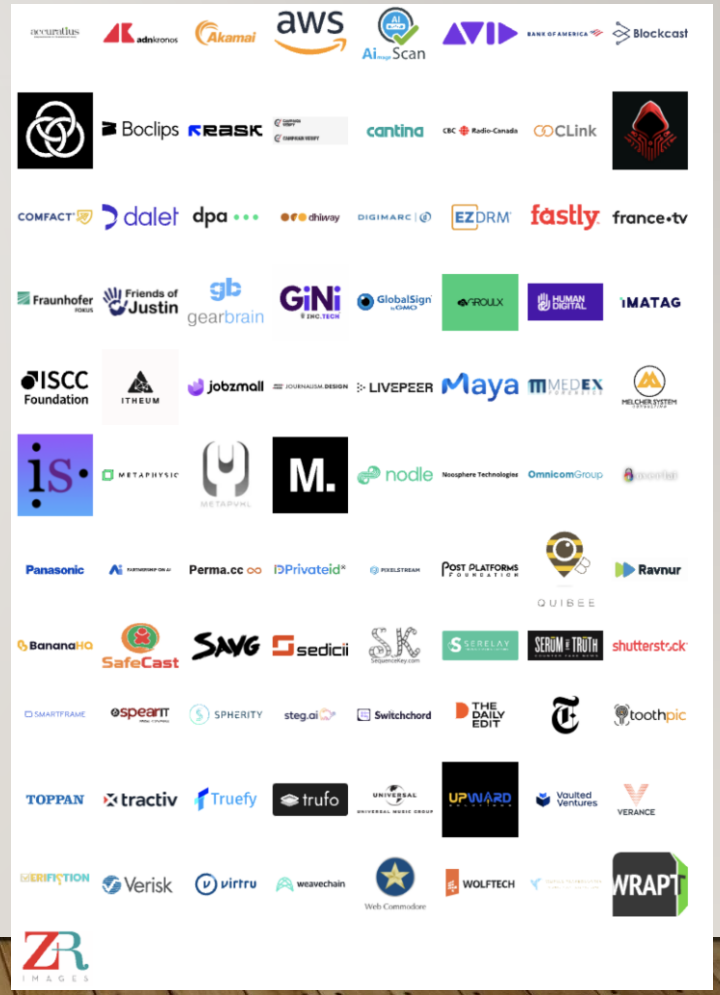
Content Credentials are implemented in several cameras, creative tools, and content platforms.

Adobe · BBC · Google · intel · Microsoft · Publicis Groupe · SONY · truepic

alteon · aws · arm · ATEME Captivate your audience · Canon · cybertrust · digicert · EAD Trust · FUTUREWEI Technologies · identity · Infosys Navigate your next · KEYFACTOR · Leica · NHK · Nikon · Numbers · polygon · ProSiebenSat.1 Media SE · Qualcomm · RIAA · WITNESS SEE IT FILM IT CHANGE IT

Liaisons

- ISO
- IPTC
- ETSI
- PDF Association

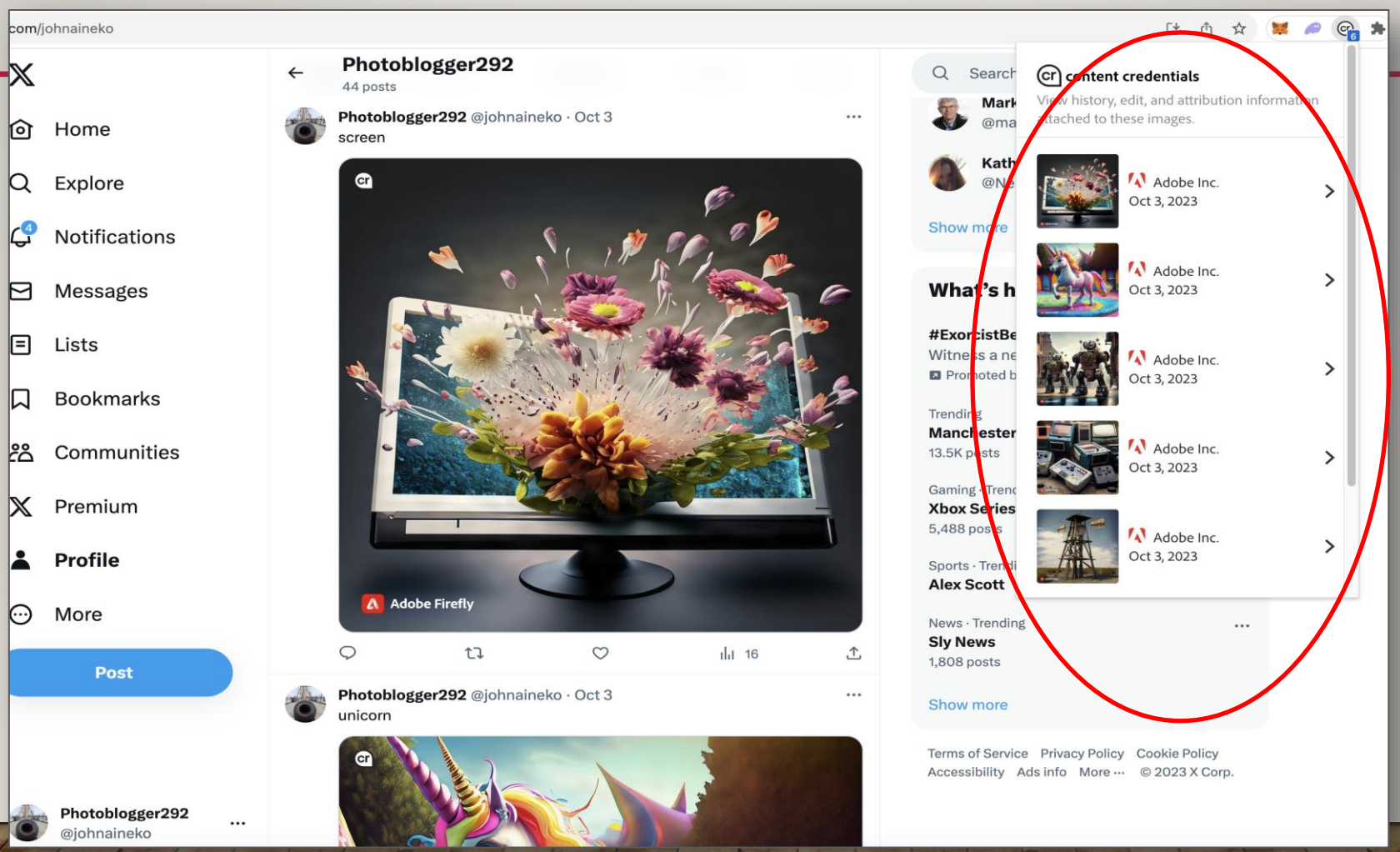


CRYPTOGRAPHY - A TRUST MODEL

- Modelled on the same approach as PDF and the Web
- Cryptographic foundation
  - Hard bindings between metadata and content (e.g., SHA256, SHA3,…)
  - X.509 certificates for signing
  - Certificate authorities and trust lists
  - Hardware attestation for cameras/mobile devices
- Soft bindings allow recovery of stripped metadata

DURABLE CONTENT CREDENTIALS

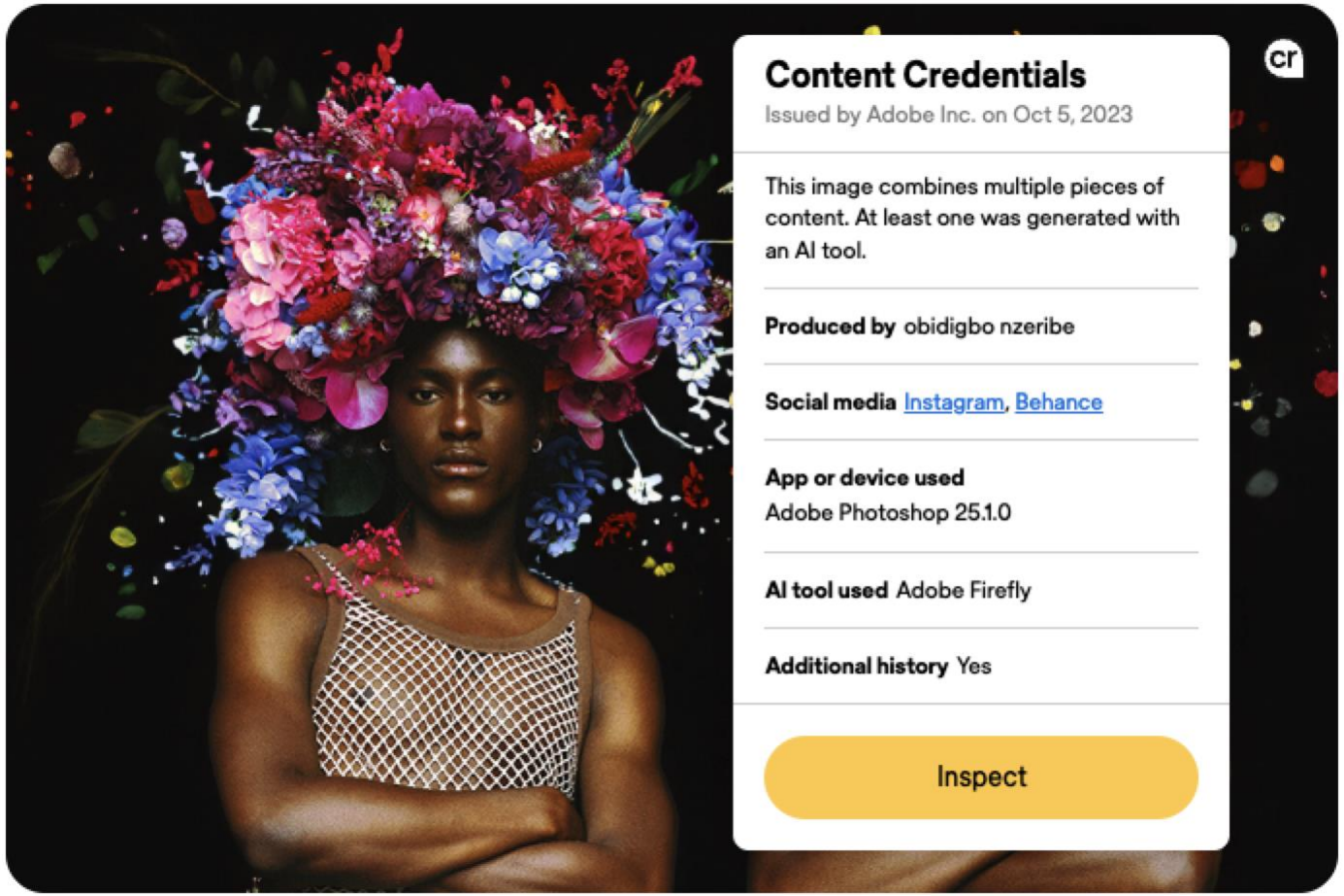
Browser detects invisible watermarks and recovers stripped content credentials from cloud

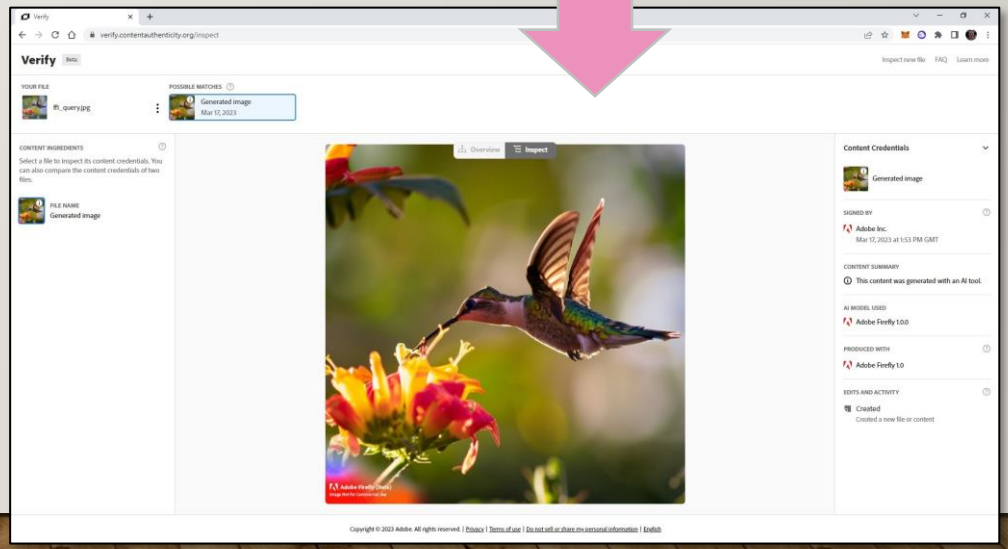


Content Credentials recovered

https://contentauthenticity.org/blog/durable-content-credentials

IDENTIFICATION OF GENERATIVE AI





TRAINING AND DATA MINING ASSERTION

- Ability to identify whether a given asset (or collection of assets) can be used in an AI/ML workflow
  - Training for Generative AI
  - Training for other forms of AI/ML
  - Use in inference
  - Use in data mining

- Building on W3C's "Text and Data Mining" CG
  - allowed
  - notAllowed
  - constrained

```
{
  "entries":
    "cawg.ai_training": {
        "use": "allowed"
    },
    "cawg.ai_generative_training": {
        "use": "notAllowed"
    },
    "cawg.data_mining": {
        "use": "constrained",
        "constraint_info": "may only be mined on days whose names end in 'y'"
    }
}
```

Detail at https://creator-assertions.github.io/training-and-data-mining/1.0/

EMBEDDED OR REFERENCED

- Content Credentials can be embedded into
  - Images (JPEG, PNG, GIF, WebP, AVIF, HEIC/HEIF, TIFF, DNG, SVG)
  - Videos (MP4, MOV, AVI, BMFF)
  - Audio (FLAC, MP3, WAV, BWF)
  - Documents (PDF, Office, EPUB)
  - Fonts (OTF, TTF)

- They can be stored separately in file systems, the cloud, DLT/Blockchains & referenced by URL, HTTP headers, file system paths and more.

THANK YOU!