ACCCF / BIBLIOTHEK FÜR ANGEWANDTES WISSEN

06

BAND

Originalität, Struktur, Kontinuität und Herkunft

Spanische Ausgabe · 2026

Handbuch zur Authentizitätsprüfung von Audio-, Video- und Bilddateien, die mit KI erzeugt oder manipuliert wurden

Prüfmethoden, Referenzen, synthetische Inhalte und Grenzen der Schlussfolgerung

Eine Multimediadatei analysieren, ohne aus einem Detektor, einem Metadatum oder einem visuellen Eindruck automatisch ein Urteil über Authentizität, Urheberschaft oder Wahrheit abzuleiten.

Für Multimedia-Sachverständige, Rechtsanwälte, Ermittler, Journalisten, prüfende Personen und Verantwortliche für die Erhaltung. Die Analyse von Sprechern, Gesichtern, Fotogrammetrie oder sensiblen Inhalten erfordert Spezialisierung und zusätzliche Kontrollen.

Redaktionelle Koordination: Jocsan Laguna · Consejo Americano de Ciberseguridad y Cómputo Forense

Allgemeine technische Anleitung und offenes Bildungsmaterial. Diese Unterlagen ersetzen keine Rechtsberatung oder forensische Begutachtung und enthalten keine Anleitung zum unbefugten Zugriff auf Systeme. Beispiele und Daten sind fiktiv; die Abbildungen sind redaktionelle Rekonstruktionen.

Inhalt

Die sichtbare Seitenzählung entspricht der PDF-Ausgabe. Word kann dieses Inhaltsverzeichnis beim Öffnen des Dokuments aktualisieren; die interne Navigation der Überschriften bleibt erhalten.

Einleitung: Sehen ist nicht Prüfen 3
Kapitel 1. Die Authentizitätsfrage 3
1.1 Original, Kopie, Bearbeitung und Darstellung 3
1.2 Auftrag und Referenzen abgrenzen 4
Kapitel 2. Erfassung und Erhaltung 5
2.1 Originalobjekt und Versionskette 5
2.2 Extraktion von Einzelbildern, Audio und Streams 5
2.3 Sicherheit und Privatsphäre 5
Kapitel 3. Struktur, Metadaten und Chronologie 6
3.1 Container, Codec und Streams 6
3.2 Chronologie von Aufnahme, Konvertierung und Veröffentlichung 6
3.3 Fall einer abweichenden Uhrzeit 6
Kapitel 4. Technische Prüfung 7
4.1 Standbild 7
4.2 Video: Struktur und zeitliche Kontinuität 7
4.3 Audio: Signal, Umgebung und Synchronität 7
4.4 Beispiel einer scheinbar offensichtlichen Bearbeitung 8
Kapitel 5. Synthetische Inhalte und Detektoren 8
5.1 Detektoren als Hinweise, nicht als Richter 8
5.2 C2PA und andere Herkunftssignale 9
5.3 Rechtsrahmen ohne universelle Kategorien 9
Kapitel 6. Bericht und eingeschränkte Schlussfolgerung 10
6.1 Nachverfolgbarkeit jeder Prüfung 10
6.2 Wann keine Schlussfolgerung möglich ist 11
Anhang A. Protokoll und Formate 11
A.1 Entgegennahmeformular für Multimediadateien 11
A.2 Prüfungsmatrix 11
A.3 Verzeichnis abgeleiteter Dateien 12
Anhang B. Funktionaler Rechtsrahmen und abschließende Checkliste 12

Einleitung: Sehen ist nicht Prüfen

Ein Bild kann etwas zeigen, das nie geschehen ist, und eine Originaldatei einer Kamera kann eine inszenierte Szene aufzeichnen. Die Authentizitätsfrage wird nicht mit „Ich sehe es deutlich“ beantwortet. Getrennt zu prüfen ist, ob die Datei das ist, als was sie ausgegeben wird, ob sie mit dem angegebenen Verfahren erzeugt wurde, ob ihre Kontinuität erhalten ist, ob sie das Ereignis zutreffend darstellt und ob sich ihre Erstellung jemandem zurechnen lässt. Jede Frage benötigt andere Quellen und kann nur unvollständig beantwortet werden.

Die Multimedia-Analyse besteht nicht darin, einen Filter zu suchen, der „falsch“ ausgibt. Sie dokumentiert die Geschichte des Objekts und vergleicht Struktur, Inhalt, Metadaten, Referenzen und Kontext. Ein Download von einer Plattform kann Informationen verlieren und dennoch dasselbe Ereignis zeigen; eine Bearbeitung kann rechtmäßig sein; eine Komprimierung kann Artefakte erzeugen, die wie Manipulation wirken. Die Schlussfolgerung ergibt sich aus der Übereinstimmung unabhängiger Elemente und den geprüften Alternativen.

SWGDE empfiehlt mehrere Methoden zur Authentizitätsprüfung von Videos und weist darauf hin, dass eine Originaldatei eine inszenierte Szene enthalten kann. Die Audio-Leitfäden zeigen, dass jede Messung mit Unsicherheiten durch Abtastung, Komprimierung, Konfiguration und Umgebung behaftet ist. Die Analyse muss Umfang und Aussagefähigkeit offenlegen und darf kein universelles Ergebnis versprechen.[1][2]

> **Vier verschiedene Fragen**
> Ist die Datei im angegebenen Sinn original? Wurde sie verändert? Hat sich die Szene wie behauptet ereignet? Wer hat den Inhalt erzeugt oder veröffentlicht? Diese vier Fragen dürfen nicht mit einem einzigen Prozentwert beantwortet werden.

Kapitel 1. Die Authentizitätsfrage

1.1 Original, Kopie, Bearbeitung und Darstellung

Original ist eine Aussage, die Kontext benötigt. Sie kann sich auf die erste von einer Kamera erzeugte Datei, auf die von einem Anbieter übermittelte Datei oder auf eine integritätsgesicherte Kopie ab einem bekannten Zeitpunkt beziehen. Ein Export kann den Inhalt mit einer anderen Struktur erhalten; eine erneute Bildschirmaufzeichnung kann dieselbe Szene mit neuen Merkmalen zeigen; ein verbessertes Bild kann die Lesbarkeit erhöhen, ohne für jede Prüfung geeignet zu sein. Vor der Analyse wird die jeweilige Darstellungsform bezeichnet.

Erzeugung, Bearbeitung, Konvertierung und Veröffentlichung sind unterschiedliche Ereignisse. Erzeugung kann eine Aufnahme mit einem Sensor oder eine Synthese mit einem Dienst bedeuten. Eine Bearbeitung verändert Inhalt oder Abfolge. Eine Konvertierung verändert Container, Codec, Größe oder Komprimierung, ohne notwendigerweise eine Täuschung zu bedeuten. Eine Veröffentlichung fügt Konto, URL, Publikum und Datum hinzu. Bei der Erhaltung werden alle bekannten Ereignisse erfasst, ohne sie unter „manipuliert“ zusammenzufassen.

[1] SWGDE 23-V-001-1.2. Best Practices for Digital Video Authentication. Untersuchung mit mehreren Methoden, Herkunft, Struktur und Einschränkungen; eine Originaldatei einer Kamera kann eine inszenierte Szene darstellen, und eine bearbeitete Datei beweist allein keine Täuschungsabsicht. Offizielle Online-Quelle

[2] SWGDE. Best Practices for Digital Audio Authentication. Globale und lokale Analyse sowie Vergleich mit Referenzdateien; die Unsicherheit hängt von Abtastung, Komprimierung, Konfiguration und Umgebung ab. Es gibt kein universelles Maß, das Authentizität feststellt. Offizielle Online-Quelle

Behauptung	Benötigte Quelle	Was nicht daraus folgt
Kameradatei	Gerät, Struktur, Exemplar und Herkunft.	Die Szene wurde nicht inszeniert.
Bearbeitetes Video	Verlauf, Struktur, Kontinuität und Vergleich.	Betrügerische Absicht oder die Falschheit sämtlicher Inhalte.
Synthetische Inhalte	Erzeugung, Verlauf, Dienst und Referenzen.	Ein bestimmtes Werkzeug allein aufgrund des Aussehens.
Veröffentlichung durch ein Konto	URL, Konto, Datum und verfügbare Aufzeichnungen.	Der Kontoinhaber hat die Datei erstellt.
Wirkliches Ereignis	Inhalt, unabhängige Bestätigung und Umstände.	Die Originalität der Datei beweist das Ereignis.

1.2 Auftrag und Referenzen abgrenzen

Im Auftrag ist festzulegen, ob Herkunft, Kontinuität, Bearbeitung, Identifizierung, Synchronität, Inhalt oder Provenienz untersucht werden soll. Nicht alle Fragen lassen sich mit derselben Datei technisch beantworten. Steht nur ein komprimierter Download zur Verfügung, reichen die Informationen möglicherweise nicht für eine Schlussfolgerung zur Originalität aus. Dies wird zu Beginn erklärt und nicht erst am Ende, um eine bereits feststehende Antwort zu rechtfertigen.

Zu den Referenzen gehören Kameraoriginale, andere Dateien derselben Sequenz, Beispielaufnahmen desselben Geräts mit derselben Konfiguration, Veröffentlichungsversionen, Bearbeitungsprojekte und Dienstprotokolle. Das Erzeugen von Vergleichsdateien auf einem Beweismittelgerät kann dessen Inhalt verändern: Zunächst wird es gesichert und anschließend geprüft, ob ein gleichwertiges anderes Gerät verwendet werden sollte. Die Referenz muss hinsichtlich Auflösung, Codec, Beleuchtung, Umgebung und Konfiguration vergleichbar sein.

> **Ausgangsbedingung**
> Soll nachgewiesen werden, dass eine Person etwas gesagt hat, liegt aber nur ein Clip ohne Kontext vor, müssen zunächst die vollständige Datei, ihre Herkunft und Vergleichsquellen beschafft werden. Ein Gutachten zur Authentizität darf nicht allein aufgrund des äußeren Eindrucks erstellt werden.



Abbildung 1. Erzeugen, Bearbeiten, Konvertieren und Veröffentlichen sind unterschiedliche Ereignisse. Die Geschichte der Datei wird rekonstruiert, bevor ihr Inhalt beurteilt wird. Redaktionelle Rekonstruktion; stellt keinen tatsächlichen Beweis dar.

Kapitel 2. Erfassung und Erhaltung

2.1 Originalobjekt und Versionskette

Je nach Fragestellung werden die native Datei, die zeitlich benachbarte Sequenz, das Gerät oder der offizielle Export angefordert. Das empfangene Objekt wird gesichert, bevor es umbenannt, mit Bearbeitungsprogrammen geöffnet oder konvertiert wird. Das Manifest erfasst ursprünglichen Namen, Größe, Format, Empfangsdatum, Kanal, Verwahrer, Identifikator und Beziehung zu anderen Versionen. Der Hashwert wird für jedes Objekt und jeden Zeitpunkt berechnet; er beweist nicht die dargestellte Szene.

Stammt die Datei von einer Plattform, werden URL, Konto, Veröffentlichung, sichtbares Datum, Datum und Zeitzone des Downloads, Werkzeug, gewählte Qualität und Parameter erfasst. Sofern rechtmäßig und relevant, werden auch die Seite und ihr Kontext aufbewahrt. Ein Bildschirmfoto der Seite ersetzt die Multimediadatei nicht, ebenso wenig wie die Datei beweist, wer das Konto verwaltet hat.

2.2 Extraktion von Einzelbildern, Audio und Streams

Werden Audio und Video getrennt oder Bilder extrahiert, erfolgt die Arbeit an einer kontrollierten Kopie. Sofern die Methode dies zulässt, wird der Stream ohne erneute Codierung kopiert. Ist eine Konvertierung erforderlich, wird ein für die Analyse geeignetes verlustfreies Format verwendet; Werkzeug, Version, Parameter und Ausgabe werden dokumentiert. Das extrahierte Bild ist ein abgeleitetes Objekt, kein neues Original.

SWGDE empfiehlt, Streams zu kopieren oder bei Bedarf in verlustfreie Formate zu transcodieren und gegebenenfalls die Gleichwertigkeit zu prüfen. So wird vermieden, eine neue Komprimierung als Merkmal der empfangenen Datei darzustellen. Die Namen abgeleiteter Dateien enthalten ihre Herkunft und werden nicht überschrieben.[3]

Gegenstand	Erlaubte Verwendung	Begleitende Dokumentation
Erhaltenes Original	Erhaltung und Vergleich von Referenzen.	Kanal, Datum, Verwahrer, Hashwert und Format.
Arbeitskopie	Reproduzierbare Untersuchung und Abfragen.	Ableitung und Werkzeug.
Einzelbild	Lokale visuelle Analyse oder Vergleich.	Zeitpunkt, Stream, Extraktion und Parameter.
Isolierte Audiospur	Signal- und Synchronitätsanalyse.	Streamkopie oder dokumentierte Konvertierung.
Aufgehelltes Bild	Lesen oder Präsentation, kein Ersatz des Originals.	Anpassung, Abfolge und Zweck.

2.3 Sicherheit und Privatsphäre

Die Dateien können Minderjährige, Opfer, Gesichter, Stimmen, Standorte, Dokumente oder intime Informationen enthalten. Zugriffe sowie Analyse- und Präsentationsversionen werden beschränkt. Dateien werden nicht auf Detektoren oder Online-Dienste hochgeladen, ohne Autorisierung,

[3] SWGDE 23-V-001-1.2. Best Practices for Digital Video Authentication. Untersuchung mit mehreren Methoden, Herkunft, Struktur und Einschränkungen; eine Originaldatei einer Kamera kann eine inszenierte Szene darstellen, und eine bearbeitete Datei beweist allein keine Täuschungsabsicht. Offizielle Online-Quelle

Vertraulichkeit, Aufbewahrung und Rechtsordnung zu prüfen. Ein kostenloser Prozentwert kann mit einer erneuten Verbreitung erkauft werden.

> **Laborregel**
> Führen Sie eine unbekannte Datei nicht auf einem Produktionssystem aus und leiten Sie sie nicht an eine Gruppe weiter, um Meinungen einzuholen. Verwenden Sie eine kontrollierte Umgebung und fiktive Daten zur Validierung von Werkzeugen; bewahren Sie das Objekt und beschränken Sie seine Verbreitung auf das Minimum.

Kapitel 3. Struktur, Metadaten und Chronologie

3.1 Container, Codec und Streams

Container, Codec, Dauer, Bildfrequenz, Auflösung, Kanäle, Zeitangaben, Tabellen und Struktur der Streams werden untersucht. Eine atypische Struktur kann auf eine Bearbeitung hindeuten, aber auch auf Export, Reparatur, Download oder Konvertierung. Vor der Interpretation wird mit Exemplaren derselben Familie und Konfiguration verglichen. Das Analysewerkzeug ersetzt nicht die Erläuterung des Befunds.

Das Fehlen eines Metadatums beweist keine Manipulation: Einige Plattformen entfernen Felder. Sein Vorhandensein beweist ebenfalls keine Originalität: Es kann kopiert oder geschrieben werden. Seine Bedeutung wird anhand der Geschichte der Datei bewertet. Eine kohärente interne Datumsangabe kann mit einer Sequenz vereinbar sein und das Ereignis dennoch nicht belegen, wenn die Uhr falsch eingestellt oder die Szene inszeniert war.

3.2 Chronologie von Aufnahme, Konvertierung und Veröffentlichung

Die Chronologie erfasst ursprüngliche Datumsangabe, Erzeuger, Zeitzone und Genauigkeit. Die Kamerazeit kann ohne Zeitzone vorliegen; das Download-Datum gehört zu einem anderen Ereignis; das Veröffentlichungsdatum kann vom Server abhängen; das Bearbeitungsdatum kann sich auf das Projekt oder den Export beziehen. Nicht alle Angaben werden so geordnet, als beschrieben sie dasselbe Geschehen. Die Sequenz bewahrt Unsicherheit und widersprüchliche Daten.

Die Dateinamen IMG_0041, IMG_0042 und IMG_0043 können Hinweise auf eine Abfolge geben; Importe, zurückgesetzte Zähler und Umbenennungen können diesen Rückschluss jedoch entkräften. Miniaturansichten, Inhalt, Metadaten, Sicherungskopien, Anwendungsprotokolle und benachbarte Dateien werden geprüft. Eine Lücke in der Namensfolge beweist keine Löschung; sie kann auf ein anderes Format oder einen nicht einbezogenen Ordner zurückzuführen sein.

3.3 Fall einer abweichenden Uhrzeit

Ein fiktives Video zeigt eine Uhr mit 18:42; eine Anklage behauptet, die Aufnahme sei um 20:42 erfolgt. Die Methode erklärt dies nicht sofort zur Fälschung und akzeptiert 18:42 auch nicht als absolute Uhrzeit. Geprüft werden die Uhr in der Szene, der Zähler des Geräts, die Zeitzone, Metadaten, Sequenz, eine frühe Veröffentlichung, Belege, andere Kameras und Zeugenaussagen. Die Abweichung kann auf einer Umrechnung, einer falsch eingestellten Uhr oder einer schwerwiegenderen Inkonsistenz beruhen.

> **Korrekte Formulierung**
> „Die Datei enthält eine sichtbare Uhr mit dem Wert 18:42 und ein internes Feld ohne angegebene Zeitzone. Die verfügbaren Quellen erlauben keinen Abgleich dieses Werts mit den behaupteten 20:42. Vor der Festlegung der Ereigniszeit sind Synchronisierung und unabhängige Bestätigung erforderlich.“

Kapitel 4. Technische Prüfung

4.1 Standbild

Dimensionen, Format, Struktur, Miniaturansichten, Sequenz, Komprimierung, Rauschen, Ränder, Beleuchtung, Perspektive und Kontinuität mit anderen Dateien werden geprüft. Eine auffällige Linie kann ein Komprimierungsartefakt sein; ein scheinbar unvereinbarer Schatten kann auf mehrere Lichtquellen oder die Perspektive zurückzuführen sein; ein erzeugtes Bild weist möglicherweise nicht die typischen Fehler auf, die die Öffentlichkeit erwartet. Die visuelle Analyse gibt Anhaltspunkte für Prüfungen, ersetzt sie aber nicht.

Vergleiche erfolgen mit dem Originalbild und eindeutig gekennzeichneten abgeleiteten Dateien. Kontrastverbesserung oder Vergrößerung kann Details sichtbar machen, aber auch Artefakte erzeugen oder verstärken. Der Bericht dokumentiert die Anpassungen und stellt die bearbeitete Version nicht als Original dar. Die Identifizierung einer Person anhand des Gesichts erfordert ein spezialisiertes Verfahren und kann nicht aus einer bloßen Ähnlichkeit abgeleitet werden.

4.2 Video: Struktur und zeitliche Kontinuität

Einzelbilder, Zeitangaben, Duplikate, Beziehungen zwischen Szenen, Audio-Synchronität, Komprimierung, Kamerawechsel und physische Kontinuität werden geprüft. Ein Sprung kann auf einer rechtmäßigen Aufnahmepause oder einem geräteseitigen Übergang beruhen; das Fehlen eines Sprungs beweist nicht, dass keine Bearbeitung stattfand. Globale und lokale Analysen werden mit Referenzen kombiniert.

SWGDE beschreibt Korrelations-, Sensor-, Farb-, Doppelkomprimierungs- und andere Analysen mit ihren Bedingungen und Grenzen. Sensorrauschen ist bei ungeeigneter Beleuchtung oder Auflösung möglicherweise kaum verwertbar; Doppelkomprimierung erklärt allein nicht den Grund. Die Schlussfolgerung muss angeben, welche Methode angewandt wurde, welches Ergebnis sie lieferte und welche Alternativen weiterhin möglich sind.[4]

4.3 Audio: Signal, Umgebung und Synchronität

Sofern der Auftrag dies zulässt, wird die gesamte Datei angehört und vermessen: Kontinuität, Umgebung, Schnitte, Echo, Rauschen, Frequenz, Sättigung, Kanäle, Synchronität und Beziehung zum Video. Ein Umgebungswechsel kann durch tatsächliche Bewegung entstehen; ein Schnitt kann auf einer Netzunterbrechung beruhen; eine identische Stimme kann geklont oder eine erneut verwendete Aufnahme sein. Das menschliche Gehör liefert eine Beobachtung, keine ausreichende Messung.

Die SWGDE-Leitfäden unterscheiden globale und lokale Analysen und empfehlen Referenzdateien mit geeigneter Konfiguration. DC Offset, Komprimierung, Spektrum oder ENF liefern keine isolierten Urteile; jede Methode hat Einsatzbedingungen und Unsicherheiten. Die Sprecheridentifizierung ist eine eigenständige Disziplin und darf nicht mit einem automatischen Vergleichswerkzeug improvisiert werden.[5]

[4] SWGDE 23-V-001-1.2. Best Practices for Digital Video Authentication. Untersuchung mit mehreren Methoden, Herkunft, Struktur und Einschränkungen; eine Originaldatei einer Kamera kann eine inszenierte Szene darstellen, und eine bearbeitete Datei beweist allein keine Täuschungsabsicht. Offizielle Online-Quelle

[5] SWGDE. Best Practices for Digital Audio Authentication. Globale und lokale Analyse sowie Vergleich mit Referenzdateien; die Unsicherheit hängt von Abtastung, Komprimierung, Konfiguration und Umgebung ab. Es gibt kein universelles Maß, das Authentizität feststellt. Offizielle Online-Quelle

4.4 Beispiel einer scheinbar offensichtlichen Bearbeitung

Ein fiktives Video scheint vor dem Zerbrechen eines Spiegels seine Kontinuität zu verlieren. Die erste Fassung enthält einen Bildschnitt; die Originaldatei der Kamera zeigt eine automatische Unterbrechung aufgrund des Aufnahmelimits, und die nächste Datei enthält die Fortsetzung. Wird nur die erste Datei geprüft, kann eine absichtliche Löschung vermutet werden; die vollständige Sequenz zeigt, dass ein Segment aus einem anderen Grund fehlt. In einem anderen Fall verhindert das fehlende Segment die Rekonstruktion des Ereignisses, was ausdrücklich erklärt werden muss.

> **Lehre**
> Eine Anomalie erfordert eine verifizierte Erklärung. Mögliche Ursachen sind Bearbeitung, Pause, Segmentierung, Codec oder Export. Ihre Bedeutung für den Fall hängt von der vollständigen Sequenz ab, nicht davon, wie dramatisch der Schnitt wirkt.

Die Analyse vergleicht mehrere Indizien und ihre Grenzen ACCCF · REDAKTIONELLE REKONSTRUKTION · FIKTIVE DATEN

Es gibt kein universelles Maß für Authentizität

Dimension	Was beobachtet wird	Warum es nicht reicht
Container	Codec, Dauer, Streams und Struktur.	Kann sich beim legitimen Export ändern.
Frames	Kontinuität, Duplikate und zeitliche Beziehungen.	Natürliche Schnitte und Komprimierung können die Analyse beeinflussen.
Audio	Wellenform, Spektrum, Umgebung und Synchronisation.	Abtastung, Kanal und Bearbeitung können die Analyse beeinflussen.
Metadaten	Produzent, Felder und Sequenz.	Sie sind veränderbar und können fehlen.
Referenz	Exemplare desselben Geräts oder derselben Version.	Konfiguration und Szene müssen vergleichbar sein.

Die Abbildung erläutert Entscheidungen und Zusammenhänge; sie stellt keine Beweise aus einem echten Fall dar.

Abbildung 2. Die Analyse vergleicht mehrere Indizien und ihre Grenzen. Es gibt kein universelles Maß für Authentizität. Redaktionelle Rekonstruktion; stellt keinen tatsächlichen Beweis dar.

Kapitel 5. Synthetische Inhalte und Detektoren

5.1 Detektoren als Hinweise, nicht als Richter

Ein Detektor kann einen Score für synthetische Inhalte erzeugen; seine Leistung hängt jedoch von Training, Version, Format, Komprimierung, Zuschnitt, erneuter Aufnahme und Inhaltsart ab. Ein positives Ergebnis kann falsch sein; ein negatives kann eine Manipulation übersehen. Werkzeug, Version, Konfiguration, exaktes Objekt, Datum und Grenzen werden dokumentiert. Nicht nur der Prozentwert wird veröffentlicht.

Vor der Nutzung eines externen Dienstes wird geprüft, ob die Datei weitergegeben werden darf. Eine lokale Analyse kann die Offenlegung reduzieren, erfordert aber ebenfalls eine Validierung. Der Detektor gibt Hinweise auf die nächsten Prüfschritte: Quelldatei, Verlauf, Referenzdatei, Projekt, Veröffentlichung oder Generierungsdienst. Er ersetzt keine dieser Quellen.

5.2 C2PA und andere Herkunftssignale

C2PA definiert Manifeste, Aussagen, Signaturen und kryptografische Bindungen an Inhalte, um deren Herkunft zu dokumentieren. Ein gültiger C2PA-Nachweis kann belegen, dass bestimmte Angaben signiert und in einem kompatiblen Prozess mit dem Asset verknüpft wurden. Er beweist weder, dass die Szene stattgefunden hat, noch dass jede Angabe des Erzeugers wahr ist. Das Fehlen eines solchen Nachweises beweist keine Fälschung.[6]

Bei der Prüfung werden Manifest, Signaturinhaber, Bestandteile, Validierungsstatus, Änderungen, Spezifikationsversion und Werkzeug erfasst. Wurde das Asset exportiert, ohne den C2PA-Nachweis zu erhalten, wird diese Einschränkung dokumentiert und nach einer früheren Version gesucht. Wasserzeichen und Metadaten ergänzen die Prüfung, ersetzen aber weder Kontext noch Originaldatei.

5.3 Rechtsrahmen ohne universelle Kategorien

Die juristische Analyse unterscheidet Einwilligung, Identität, Verwendung, Verhalten, Datum und Rechtsregime. In Mexiko behandeln die Artikel 199 Octies und 199 Nonies des Bundesstrafgesetzbuchs bestimmte Verhaltensweisen mit intimen Inhalten ohne Einwilligung, auch wenn das Material nicht der identifizierten Person entspricht. In der Europäischen Union regelt Artikel 50 der KI-Verordnung die Transparenz bestimmter Deepfakes und sieht Anpassungen für kreative Werke und Fiktion vor. Keine dieser Regelungen entspricht einem weltweiten Verbot jeglicher KI.[7][8]

Ein satirisches, pädagogisches oder offen synthetisches Werk darf nicht ohne Prüfung seines Kontexts als täuschende Darstellung behandelt werden. Umgekehrt klärt die Kennzeichnung „ist KI“ weder Einwilligung noch Schaden, Eigentum oder Verwendung. Die technische Schlussfolgerung beschränkt sich auf Herkunft und Veränderungen; die juristische Analyse erfolgt anhand der einschlägigen Norm und der Tatsachen.

> **Fiktiver Fall**
> Eine Veröffentlichung zeigt eine Person, deren Stimme als geklont ausgewiesen ist. Die Datei enthält ein Generierungsmanifest und eine sichtbare Beschreibung der Produktion. Die Authentizität der Stimme als natürliche Stimme wird begründet verneint, die Veröffentlichung verschweigt ihre Synthese jedoch nicht. Fragen der Autorisierung, Verwendung und Wirkung auf das Publikum bleiben gesondert zu prüfen.

[6] Coalition for Content Provenance and Authenticity. C2PA Technical Specification 2.3 (05-01-2026). Herkunft, Manifeste, Aussagen und kryptografische Bindung an den Inhalt. Das Fehlen von C2PA-Nachweisen beweist keine Fälschung, und ihr Vorhandensein beweist nicht die Wahrheit der Szene. Offizielle Online-Quelle

[7] Mexiko. Código Penal Federal, Artikel 199 Octies und 199 Nonies, Zusammenstellung mit der Reform vom 13-03-2026: bestimmte Verhaltensweisen mit sexuell intimen Inhalten ohne Einwilligung, auch wenn das Material nicht der identifizierten Person entspricht. Offizielle Online-Quelle

[8] Verordnung (EU) 2024/1689 über künstliche Intelligenz, Artikel 50, konsolidierter Text vom 27-07-2026: Transparenz für bestimmte Deepfakes und Anpassungen für kreative, satirische, künstlerische oder fiktive Werke. Offizielle Online-Quelle



Abbildung 3. Überprüfbare Herkunft bedeutet nicht, dass die Szene wahr ist. C2PA und Detektoren haben unterschiedliche Funktionen bei der Prüfung. Redaktionelle Rekonstruktion; stellt keinen tatsächlichen Beweis dar.

Kapitel 6. Bericht und eingeschränkte Schlussfolgerung

6.1 Nachverfolgbarkeit jeder Prüfung

Der Bericht bezeichnet Auftrag, Objekte, Darstellungen, Werkzeuge, Versionen, Parameter, Referenzdateien, Abfragen und Ergebnisse. Jeder Befund verweist auf die analysierte Datei, den Zeitpunkt oder Bereich und gegebenenfalls auf die abgeleitete Abbildung. Bilder werden mit ihrer Quelle und den verwendeten Anpassungen ausgewiesen. War eine Prüfung nicht möglich, werden Grund und Auswirkung auf die Schlussfolgerung erläutert.

Beobachtung, Messergebnis, Inferenz und Schlussfolgerung werden unterschieden. „Das Einzelbild weist eine Diskontinuität auf“ ist eine Beobachtung; „die Korrelation nimmt in diesem Bereich ab“ ist ein Messergebnis; „dies ist mit einer Bearbeitung vereinbar“ ist eine Inferenz; „die Datei wurde von einer Person hergestellt“ erfordert eine andere Quelle. Die Formulierung hält diese Ebenen auseinander, damit der Leser den Schlussübergang nachvollziehen kann.

Ergebnis	Zulässige Formulierung	Informationen, die sie verändern können
Übereinstimmender Hashwert	Das Objekt wurde zwischen zwei Prüfungen nicht verändert.	Identifizierungs- oder Algorithmusfehler.
Atypische Struktur	Mit Bearbeitung oder Konvertierung vereinbar; erfordert eine Referenz.	Ursprünglicher Export des Geräts.
Positives Detektorergebnis	Orientierendes Indiz mit Version und Grenzen.	Original, Verlauf oder unabhängige Analyse.
Gültiger C2PA-Nachweis	Signierte Angaben, die mit dem Asset verknüpft sind.	Zertifikat, Beweismittelkette oder ursprünglich falscher Inhalt.
Keine Schlussfolgerung	Unzureichende Daten für Originalität oder Szene.	Native Datei und vergleichbare Exemplare.

6.2 Wann keine Schlussfolgerung möglich ist

Das Ausbleiben einer abschließenden Schlussfolgerung ist keine Niederlage: Es verhindert, dass aus einem Verdacht eine schädliche öffentliche Behauptung wird. Steht nur eine komprimierte Kopie ohne Verlauf und Referenzen zur Verfügung, kann der Bericht die Beobachtungen beschreiben und die benötigte Quelle benennen. Die Lücke wird weder mit wissenschaftlich klingender Sprache noch mit einer Sammlung von Filtern gefüllt.

Die unabhängige prüfende Person versucht, die Abfragen zu reproduzieren und alternative Erklärungen zu finden. Sie prüft außerdem, ob Rekonstruktionen nicht als tatsächliche Beweise dargestellt werden und ob Abbildungen keine Informationen verbergen. Ändert eine neue Quelle die Schlussfolgerung, wird die Analyse aktualisiert, ohne den Versionsverlauf zu löschen.

> **Fazit**
> Ziel ist nicht, um jeden Preis ein Urteil zu erhalten. Ziel ist, genügend Quellen und methodische Informationen zu erhalten, damit die Schlussfolgerung auch einer Überprüfung standhält, die den ersten Eindruck nicht teilt.

Anhang A. Protokoll und Formate

A.1 Entgegennahmeformular für Multimediadateien

Fiktives Manifest

```
Objekt / ID: DEMO-VID-001-R00
Ursprünglicher Name und Format: [Namen beibehalten]
Angegebene Quelle: [Kamera, Export, Plattform, Person]
Kanal und Datum des Empfangs: [EML, Link, Gerät]
URL, Konto und Veröffentlichung: [falls zutreffend]
Größe, Dauer, Auflösung und Streams: [beobachtet]
Hashwert und Algorithmus: [Objekt und Zeitpunkt]
Verwandte Versionen: [Original, Download, Kopie, Referenz]
Angegebener Verlauf: [Erzeugung, Bearbeitung, Konvertierung, Veröffentlichung]
Rechtliche Befugnis und Datenschutz: [Umfang, Beschränkungen]
Vorkommnisse: [beschädigte Datei, fehlender Codec, fehlende Angaben]
Verbleib: [gesichert, Arbeitskopie und Zugriff]
```

A.2 Prüfungsmatrix

Frage	Methode und Referenz	Ergebnis	Grenze / nächste Quelle
Ist die Struktur vereinbar?	[Container, Referenzdatei]	[Beobachtung]	[Mögliche Umwandlung]
Liegt zeitliche Kontinuität vor?	[Einzelbilder, Sequenz]	[Beobachtung]	[Pause oder Bearbeitung]
Ist das Audio kohärent?	[Signal, Spektrum, Referenz]	[Beobachtung]	[Umgebung, Abtastung]
Herkunft?	[C2PA, Vorgeschichte, Aufzeichnungen]	[Zustand]	[Fehlen beweist keine Fälschung]
Ist die Szene real?	[Unabhängige Bestätigung]	[Vereinbar / ungewiss]	[Datei allein genügt nicht]
Urheberschaft?	[Konto, Projekt, Gerät]	[Verknüpfung]	[Person nicht automatisch bestimmen]

A.3 Verzeichnis abgeleiteter Dateien

Abgeleitete Datei	Quelle	Methode und Parameter	Erlaubte Verwendung
Arbeitskopie	DEMO-VID-001-R00	Überprüfte Kopie und zugehöriger Hashwert.	Untersuchung, ohne das Original zu verändern.
Einzelbild 00:12:04	Kopie W01	Verlustfreie Extraktion; Werkzeug und Version.	Lokaler Vergleich.
Isolierte Audiospur	Kopie W01	Streamkopie oder dokumentierte Konvertierung.	Signalanalyse.
Aufgehelltes Bild	Einzelbild D01	Dokumentierter Kontrast und Zuschnitt.	Präsentation, kein Ersatz.
Bericht und Anhänge	Alle Objekte	Manifest, Abfragen und Version.	Unabhängige Überprüfung.

Anhang B. Funktionaler Rechtsrahmen und abschließende Checkliste

Ein elektronisches Dokument kann zugelassen werden, ohne dass damit die Frage seiner Authentizität entschieden ist. In Mexiko sind CCom, je nach Übergangsregelung CFPC/CNPCF sowie NOM-151 für die Aufbewahrung im jeweiligen Bereich zu prüfen; Peru trennt Signatur, Verfahren und Archivierung; Chile unterscheidet Signatur und Datum; Argentinien gewichtet die Zuverlässigkeit; Kolumbien und Ecuador verlangen einen Aufbewahrungskontext; Spanien verbindet eIDAS, LEC und Vertrauensdienste. Diese Funktionen werden gegebenenfalls durch besondere Regeln zu KI, intimen Inhalten und Datenschutz ergänzt.[9][10][11][12][13][14][15][16][17][18][19]

Vor der Ausgabe	Überprüfung
Frage	Originalität, Veränderung, Szene, Urheberschaft oder Veröffentlichung?
Quelle	Sind native Datei, Verlauf, Sequenz, Referenzdatei und Kontext verfügbar?
Methode	Sind Werkzeuge, Versionen, Parameter und abgeleitete Dateien dokumentiert?

[9] Código de Comercio de México, Artikel 89–94 und 1205: Neutralität, Zurechnung, Schriftform, Original, Integrität, Zugänglichkeit und Zulassung von Datennachrichten. Offizielle Zusammenstellung. Offizielle Online-Quelle

[10] Código Nacional de Procedimientos Civiles y Familiares, Artikel 348–350. Zusammenstellung mit der Reform vom 15-01-2026. Die Anwendung erfolgt schrittweise und hängt von entsprechenden amtlichen Feststellungen ab. Offizielle Online-Quelle

[11] NOM-151-SCFI-2016, Aufbewahrung und Digitalisierung von Datennachrichten, veröffentlicht am 30-03-2017. Anforderungen an Bescheinigung, Integrität, Zugänglichkeit und elektronischen digitalen Fingerabdruck. Offizielle Online-Quelle

[12] Peru. Código Procesal Civil, Artikel 188–197 und 245.5: Zweck, Rechtmäßigkeit, Beweismittel, Beweislast, Beweiswürdigung und Datumsangaben durch technische Mittel. Offizielle Online-Quelle

[13] Chile. Ley 19.799 über elektronische Dokumente und elektronische Signaturen, Artikel 1–5: Gleichwertigkeit, Schriftform, einfache/fortgeschrittene elektronische Signatur, Datum und Beweiswert. Offizielle Online-Quelle

[14] Argentinien. Código Civil y Comercial, Artikel 318–319: Korrespondenz mit beliebigen Mitteln und Bewertung der Zuverlässigkeit von Trägern und technischen Verfahren. Offizielle Online-Quelle

[15] Kolumbien. Ley 527 de 1999, Artikel 5–13, 16–25 und 28: Datennachrichten, Schriftform, Original, Integrität, Zulässigkeit, Aufbewahrung, Versand, Empfang und digitale Signatur. Offizielle Online-Quelle

[16] Ecuador. Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, Ley 67, Artikel 2, 6–8, 10–16: Gleichwertigkeit, Schriftform, Original, Aufbewahrung, Herkunft, Versand, Empfang und elektronische Signatur. Offizielle Online-Quelle

[17] Spanien. Ley de Enjuiciamiento Civil, Artikel 326 und 384: private Dokumente, Anfechtung, Instrumente zur Archivierung, Kenntnisnahme oder Wiedergabe von Daten, Prüfung, Verwahrung und vernunftgeleitete Beweiswürdigung. Offizielle Online-Quelle

[18] Mexiko. Código Penal Federal, Artikel 199 Octies und 199 Nonies, Zusammenstellung mit der Reform vom 13-03-2026: bestimmte Verhaltensweisen mit sexuell intimen Inhalten ohne Einwilligung, auch wenn das Material nicht der identifizierten Person entspricht. Offizielle Online-Quelle

[19] Verordnung (EU) 2024/1689 über künstliche Intelligenz, Artikel 50, konsolidierter Text vom 27-07-2026: Transparenz für bestimmte Deepfakes und Anpassungen für kreative, satirische, künstlerische oder fiktive Werke. Offizielle Online-Quelle

Vor der Ausgabe	Überprüfung
Alternativen	Wurden Konvertierung, Pause, inszenierte Szene und rechtmäßige Bearbeitung geprüft?
KI	Werden Detektoren mit ihren Grenzen und C2PA mit seinem Aussageumfang interpretiert?
Datenschutz	Wurde die Datei nur mit Autorisierung und auf das Mindestmaß beschränkt geteilt?
Schlussfolgerung	Lässt sich jede Aussage auf eine Quelle zurückführen und sind ihre Grenzen angegeben?

Fazit

Authentizität wird nicht anhand von Ähnlichkeit oder Technologieangst bewertet. Geprüft wird mit Dateien, Verlauf, Vergleichen und einer Schlussfolgerung, die ihre eigenen Grenzen anerkennt.