c't magazin für computer technik

# KI-manipulierte Bilder mit OSINT-Methoden entlarven

| 30.03.2026 15:00 Uhr Wilhelm Drehling

**Manchmal ist es bei Recherchen notwendig, Bilder zu analysieren, etwa um den Aufnahmeort zu bestimmen oder Änderungen am Bild nachzuweisen.**

Bildanalysen gehören zum täglichen Brot beim Sammeln von Informationen aus öffentlichen, frei verfügbaren Quellen (Open Source Intelligence, OSINT).

Typische Aufgaben sind, Orte von Aufnahmen ausfindig zu machen, mögliche Manipulationen am Bild aufzudecken oder die Quellen zu verifizieren. Vor allem mit dem Aufkommen von KI-manipulierten Bildern sind Änderungen nicht immer leicht zu erkennen.

MEHR ZUM THEMA KÜNSTLICHE INTELLIGENZ (KI)

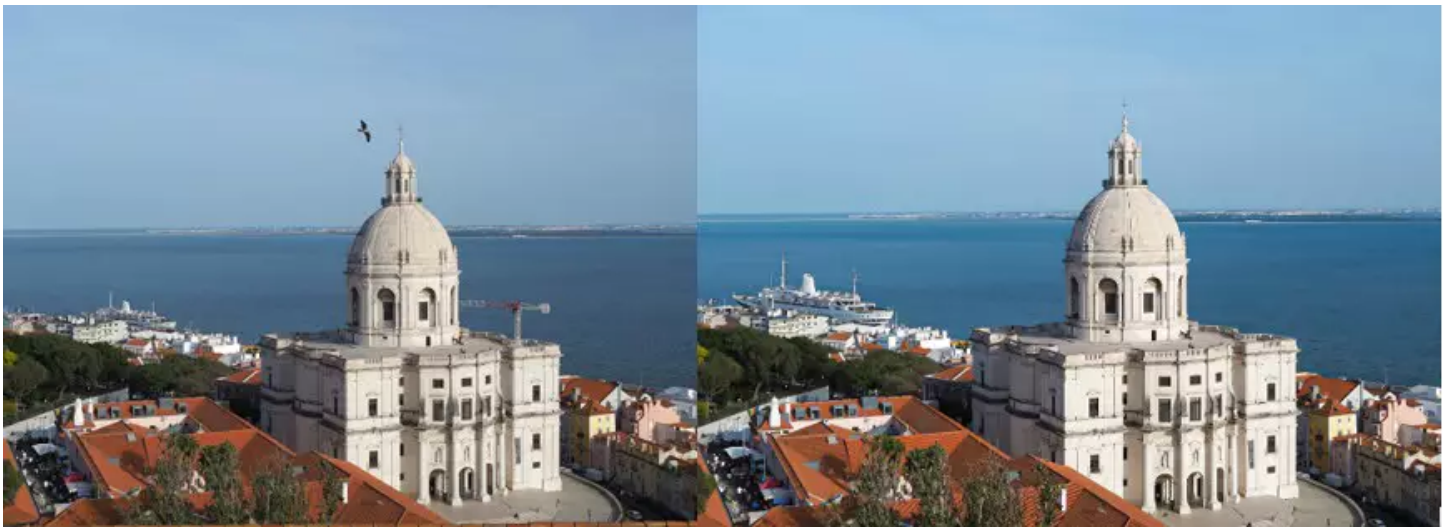
**KI-manipulierte Bilder mit OSINT-Methoden entlarven [1]**

**Schluss mit Fake News: KI-Faktenchecks gezielt per Bookmarklet auslösen [2]**

**Eigene KI-Bildmaschine: So läuft Flux lokal auf dem PC [3]**

**Hannover Messe verspricht mehr künstliche Intelligenz und KI-gesteuerte Roboter [4]**

Wir zeigen am Beispiel eines Bildes, das wir im November 2024 aufgenommen haben, wie man Änderungen, die etwa mit KI-Hilfe eingebaut wurden, entdeckt. Das Original sowie die bearbeitete Version finden Sie als Download **hier [5]** (original.jpg) und **hier [6]** (fake.png).



Wir haben das Bild oben von November 2024 mit KI bearbeitet. Links sieht man das Original. Rechts die bearbeitete Version. Ihre Aufgabe: Finden Sie alle Ungereimtheiten im Bild.
(Bild: Wilhelm Drehling)

## Metadaten

Bevor es ans Bild selbst geht, lohnt es sich, einen Blick in die Innereien der Datei zu werfen. Egal, ob Sie ein Foto mal eben schnell mit dem Smartphone knipsen oder mit einer professionellen Kamera unterwegs sind, fast jedes Bild enthält Informationen zu den genauen Kameraeinstellungen in den sogenannten Metadaten. Diese können von nur wenigen Angaben wie Bildgröße, Name, Uhrzeit und Kamerahersteller bis zu den genauen Einstellungen und sogar Geodaten zum Standort hinausgehen.

Auch wenn diese Daten nicht in Stein gemeißelt sind und Fachkundige die hinterlegten Informationen umschreiben können, wäre es töricht, sich die Daten nicht anzuschauen. Je nach Betriebssystem des Gerätes, mit dem man das Bild betrachtet, versteckt sich die Auflistung der Metadaten etwas unterschiedlich: Am PC finden Sie sie mit Rechtsklick auf das Bild unter einem Tab wie Informationen, Einstellungen oder Eigenschaften.

Anstatt händisch die Metadaten zu durchsuchen, bietet es sich an, ein Kommandozeilenwerkzeug wie

**exiftool (Download) [7]** zu verwenden, das die Ergebnisse nicht nur hübsch in der Konsole auflistet, sondern auch weitaus mehr Daten aus dem Bild extrahiert als ein typisches Eigenschaften-Fenster anzeigt. Exiftool ist Open Source, funktioniert für sehr viele Bildformate und steht sowohl unter Windows ( `winget install exiftool` ), als auch unter Linux (etwa `sudo apt install exiftool` ) und macOS ( `brew install exiftool` ) zur Verfügung.

```
Filter                          : Adaptive
Interlace                       : Noninterlaced
Pixels Per Unit X               : 11811
Pixels Per Unit Y               : 11811
Pixel Units                     : meters
XMP Toolkit                     : Adobe XMP Core 9.1-c003 79.9690a87fc, 2025/03/06-20:50:16
Digital Image GUID              : 6e36620b-724f-4387-b5f1-a7ac1b39c94b
Digital Source Type             : http://cv.iptc.org/newscodes/digitalsourcetype/trainedAlgorithmicMedia
Create Date                     : 2025:05:09 11:33:47+02:00
Modify Date                     : 2026:03:27 11:21:04+01:00
Metadata Date                   : 2026:03:27 11:21:04+01:00
Creator Tool                    : Adobe Photoshop 27.1 (Macintosh)
Format                          : image/png
```

Für unser Original liefert exiftool zahlreiche Informationen zur genauen Kamerakonfiguration zum Zeitpunkt der Aufnahme. Beim Fake dagegen entblößt es die Bearbeitung durch eine KI (Digital Source Type).

Nach der Installation spuckt der Befehl `exiftool <bild>` alle Metadaten aus. Für das Original erschlägt das Tool einen mit allen möglichen Kameraeinstellungen Abgesehen von Größe (3,2 MByte), Pixelauflösung (4608 × 3456) und genauer Uhrzeit (2024:11:23 17:06:30+01:00), verrät es auch einiges über das Kameramodell (Olympus E-M10 Mark III), dem Objektiv (Panasonic Lumix G 25mm F1.7) und der genauen Konfiguration der Aufnahme wie ISO-Einstellung und so weiter. Beim Fake dagegen offenbart exiftool, dass eine generative KI am Werk war, und zwar innerhalb von Adobe Photoshop 27.1.

Ein weiteres nützliches Werkzeug ist **binwalk**. Unter Windows ist es umständlich zu installieren, wir empfehlen daher, auf das Windows-Subsystem für Linux (WSL) auszuweichen ( `wsl --install` installiert Ubuntu), das den Zugriff auf eine Linux-Konsole eröffnet. Linuxer installieren binwalk via `apt` , macOS-Nutzer per `brew` .

Eigentlich ist binwalk für die Analyse von Programmdateien gedacht, weil es den genauen Aufbau der Datei aufdröselt. Lässt man es auf Bilder los, kann es darin versteckte Dateien entblößen, die durch bloßes Betrachten des Bildes niemals ans Tageslicht gelangen wären. Dateien in Bildern zu verstecken, ist eine Art steganografisches Mittel, um etwa Programme unbemerkt zu verbreiten. Im **Hacking-Walkthrough zu Necromancer [8]** haben wir mit exiftool und binwalk Bilder analysiert und gezeigt, wie man etwa eine Zip-Datei in einem Bild findet und anschließend extrahiert.

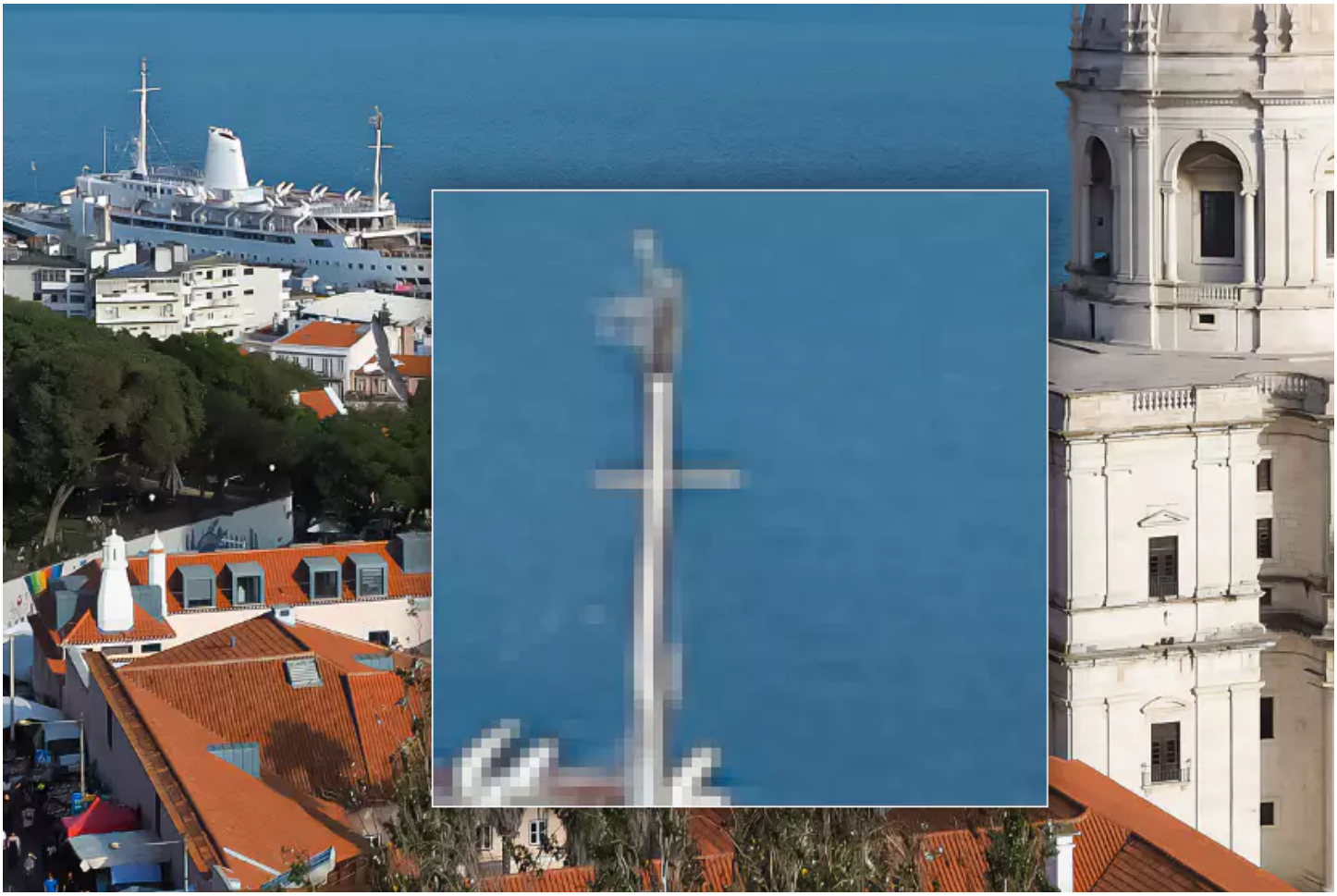
**[9]**

## Manipulationen aufdecken

Auf den ersten Blick sehen viele bearbeitete Bilder echt aus, erst beim genaueren Hinschauen fallen Unstimmigkeiten auf. **Der Spiegel gab vor einigen Wochen bekannt [10]**, dass sie versehentlich KI-manipulierte Bilder veröffentlicht haben. In diesem Fall hat die Bildagentur mit KI nachgeholfen, diese aber nicht gekennzeichnet.

Nicht immer sind Manipulationen so einfach zu entdecken, wie die berühmten sechs Finger an einer Hand: Die einfachste – aber auch mühsamste – Lösung ist, das Bild ganz genau unter die Lupe zu nehmen. Hierbei hilft das online verfügbare Tool **Forensically [11]**, das zwar im Browser, aber vollständig clientseitig läuft. Über die Option „Open File“ laden Sie ein Bild hoch.

Standardmäßig läuft der Modus „Magnifier“, der den Mauszeiger in eine Art Mikroskop verwandelt. Mit diesem suchen Sie im Bild nach komischen Kanten oder verwaschenen Flächen, die ein Indiz für eine mögliche Änderung sein können. Bei von KI-manipulierten Bildern fallen meist Logikfehler auf: Etwa ein Schatten, der nicht passend zur Uhrzeit und der Sonnenposition fällt, Gegenstände, die im Hintergrund schweben, seltsame Konstruktionen oder Oberflächen, die nicht vernünftig an andere Flächen anschließen. Verpixelte Vierecke deuten meist auf eine Komprimierung hin, die etwa durch das JPEG-Format zustande kommen. Das kann dafür sprechen, dass es sich bei dem Bild nicht mehr um das Original handelt, sondern um eine Version, die schon eine Weile durch Social Media geistert.



Mit der Magnifier-Funktion von Forensically fallen beim Mast des Fake-Kreuzfahrtschiffs KI-Halluzinationen auf.

Auf der rechten Seite finden Sie viele weitere hilfreiche Funktionen, um Manipulationen aufzudecken: Mit „Noise Amplitude“ fallen Pixelflächen auf, die ein anderes Grundrauschen aufweisen, was für nachträglich eingefügte Objekte sprechen könnte. In die gleiche Kerbe schlägt „Error Level Analysis“. Unter „Meta Data“ liefert Forensically die bereits besprochenen Metadaten.

Probieren Sie ruhig einmal die Funktionen von Forensically mit unseren Bildern und mit dem vom Softwareanbieter zur Verfügung gestellten UFO-Beispielbild aus. Vor allem „Noise Amplitude“ deckt einige Schwachstellen auf: So unterscheidet sich das Rauschen zwischen dem Original und dem Fake signifikant, jegliche Tiefe im Bild geht beim Fake verloren, was auf eine Bearbeitung mit KI schließen lässt.

## KI gegen KI-Fakes

Zum Detektieren von KI-manipulierten Bildern können auch KI-Werkzeuge helfen – klar, was denn sonst. Diese sind aber mit einer gesunden Portion Skepsis zu betrachten, denn nicht alles, was die diversen verfügbaren Tools als „KI“ abstempeln, ist auch wirklich KI-generiert. Als zusätzliche Meinung ist es aber trotzdem keine schlechte Idee, solche Prüfwerkzeuge zu befragen.

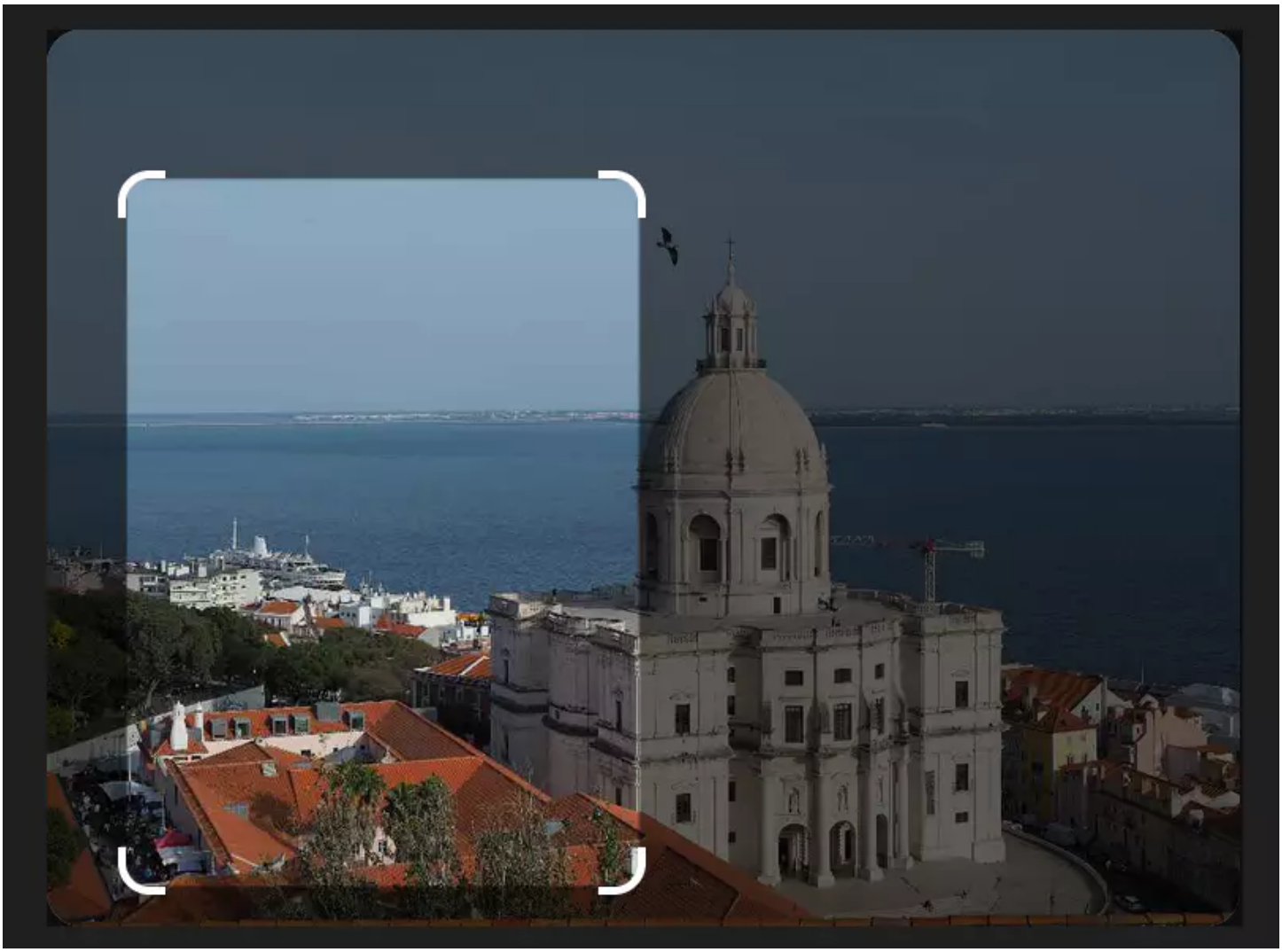
Wir haben drei Exemplare zufällig ausgewählt und ausprobiert, alle drei führen kostenlose Checks ohne Anmeldung durch: **ZeroGPT [12]**, **Decopy AI [13]** und **wasitai [14]**. Wasitai hält das Bild für echt, die anderen beiden Dienste sind da anderer Meinung und entlarven den Fake als KI-generiert.

An der Stelle sei gewarnt: Laden Sie nicht wahllos Bilder hoch, vor allem nicht, wenn sie Personen zeigen, deren Erlaubnis Sie nicht haben. Man weiß nie genau, was die zahlreichen Tools, die überall aufploppen, mit den Bildern anstellen.

## Ort herausfinden

Wer mit OSINT-Werkzeugen arbeitet, tut das oft, um Fake-Aufnahmen zu verifizieren. Dabei geht es oft darum, den tatsächlichen Ort des Gezeigten herauszufinden. So analysieren etwa **OSINT-Experten Bildmaterial vom Angriffskrieg Russlands auf die Ukraine [15]**, um Kriegsverbrechen nachzuweisen oder Propaganda zu widerlegen.

Metadaten enthalten manchmal den genauen GPS-Standort, ein Geotag, das in unserem Beispielbild fehlt. Selbst wenn es vorhanden wäre, könnte es jemand als plumpe Desinformation platziert haben. Man muss also prüfen, ob die angegebenen Daten stimmen. Daher ist es gut, wenn man die nachfolgenden Kniffe kennt, mit denen man anhand der abgebildeten Informationen auf den Ort schließen kann.



Mit dem Auswahlwerkzeug der Rückwärtsbildersuche von Google suchen Sie nach nur einem gewissen Ausschnitt.

Der erste Anlaufpunkt ist die **Rückwärtsbildersuche von Google [16]** oder die App Google Lens (alternativ eignen sich auch andere Anbieter wie Tineye oder Yandex). Dazu rufen Sie einfach Google auf und laden über das Foto-Symbol in der Suchleiste das Bild hoch. Die Bildersuche erlaubt Ihnen, das Netz nach dem ganzen Bild zu durchsuchen oder mithilfe des Zuschnittswerkzeugs nur einen bestimmten Ausschnitt auszuwählen. Nicht selten sind in Bildern auffällige Strukturen wie eine ungewöhnlich geformte Laterne, historische Fassaden oder merkwürdig bedruckte Mülleimer, die die Trefferwahrscheinlichkeit erhöhen können.

In unserem Beispiel sollte das prominente weiße Gebäude in der Mitte des Bildes ausreichen. Die Suche ergibt, dass es sich bei dem Gebäude um das Pantheon (Igreja de Santa Engrácia) in Lissabon handelt. Es gibt auch weitere Bilder, die, wie es scheint, vom selben Ort schräg oberhalb des Pantheons aufgenommen wurden. Doch von wo genau?

Wenn Sie nun Detektiv spielen wollen, könnten Sie das Pantheon über Google Maps oder einen anderen Kartenanbieter aufsuchen und schauen, welches Gebäude infrage kommen würde. Spoiler: Auffällig dabei ist die große Kirche Igreja de São Vicente de Fora, die leicht abseits steht und vom

Winkel ungefähr hinkommt. Street View räumt die letzten Zweifel aus: Eine der Blubberblasen auf der Kirche zeigt die Sicht vom Dach mit Blick auf das Pantheon – damit ist der Aufnahmeort des Fotos klar.

Bei Bildern ohne jegliche besonderen Merkmale erfordert diese Suche sehr viel Fleiß und Erfahrung: Zuerst grenzt man den ungefähren Standort ein, indem man anhand des Sonnenstands die Hemisphäre bestimmt. Weitere Hinweise liefert die Art der Vegetation, die Farbe der Straßenmarkierungen, Form der Straßenschilder, Sprache auf Schildern, Leitpfosten, Häuser, Kleidung und so weiter.

Viele Ansatzpunkte lassen sich dabei aus dem Geografie-Spiel **GeoGuessr [17]** übernehmen, das einen irgendwo auf der Welt aussetzt und in dem man anhand von Street View versuchen muss, den Standort herauszufinden. Für dieses Spiel lernen Profis tausende kleine Merkmale auswendig, wie das regional unterschiedliche Aussehen von Nummernschildern oder den Zustand des Grases, um den ungefähren Standort erraten zu können. Besonders bekannt ist etwa der YouTuber Rainbolt, der viele Videos darüber gemacht hat, wie er anhand von bestimmten Merkmalen im Bild den exakten Ort bestimmen konnte.

## Fazit der Analyse

Ein kurzes Résumee zu dem Bild: Durch exiftool kennen Sie nun die genaue Uhrzeit der Aufnahme, sowie sämtliche Kameraeinstellungen des Bildes. Mithilfe der Rückwärtsbildersuche konnten Sie den Ort der Aufnahme auf Lissabon eingrenzen, den genauen Standort verifizieren und mit Forensically feststellen, dass das Bild nachträglich verändert wurde.

Die Tipps und Tools aus diesem Artikel bilden die Grundlage, um bearbeitete Bilder zu erkennen. Es gibt zwar noch viele weitere Tricks, aber mit diesen sollten Sie ausreichend gewappnet sein, um erste Bilder zu analysieren. Übrigens: Haben Sie im Fake den versteckten Zauberwürfel gefunden? (**wid [18]**)

---

**URL dieses Artikels:**

https://www.heise.de/-11208411

**Links in diesem Artikel:**

**[1]** https://www.heise.de/hintergrund/KI-manipulierte-Bilder-mit-OSINT-Methoden-entlarven-11208411.html

**[2]** https://www.heise.de/ratgeber/Schluss-mit-Fake-News-KI-Faktenchecks-gezielt-per-Bookmarklet-ausloesen-11225498.html

**[3]** https://www.heise.de/ratgeber/Eigene-KI-Bildmaschine-So-laeuft-Flux-lokal-auf-dem-PC-11206629.html

**[4]** https://www.heise.de/hintergrund/Hannover-Messe-verspricht-mehr-kuenstliche-Intelligenz-und-KI-gesteuerte-Roboter-11185777.html

**[5]** https://ftp.heise.de/ct/listings/2026/09/original.jpg

**[6]** https://ftp.heise.de/ct/listings/2026/09/fake.png

**[7]** https://www.heise.de/download/product/exiftool-35845

**[8]** https://www.heise.de/ratgeber/Hacking-Walkthrough-Spielerisches-Training-mit-der-Necromancer-VM-7485561.html

**[9]** https://www.heise.de/ct

**[10]** https://www.spiegel.de/backstage/medien-manipulierte-fotos-in-berichten-zu-iran-entdeckt-a-f214eb7a-23dd-4d4b-b6e3-e789f495a9ec

**[11]** https://29a.ch/photo-forensics/#forensic-magnifier

**[12]** https://www.zerogpt.com/ai-image-detector

**[13]** https://decopy.ai/ai-image-detector/

**[14]** https://wasitai.com/

**[15]** https://www.heise.de/hintergrund/OSINT-Experten-Mit-Akribie-gegen-Kriegsverbrechen-und-Propaganda-7073022.html

**[16]** https://www.google.de/imghp?hl=de

**[17]** https://www.geoguessr.com/

**[18]** mailto:wid@heise.de