

Spurensuche 2.0:

Wie Künstliche Intelligenz OSINT-
Operationen transformiert



Kurzvorstellung Trainer



- 2022 gegründet
- IT-Sicherheitsberatung
- OSINT Analysen & Schulungen
- IT-Risiko- und Bedrohungsanalysen

Inhalte

1. Quellenoptimierung

- Klassische Datengewinnung
- KI gestützte Datengewinnung

2. Smarte Analyse

- Bildgeneratoren
- Daten analysieren & anreichern
- Deepfakes
- Geo-Analyse mit LLMs

Was ist Open Source Intelligence?

Open Source Intelligence (OSINT) bezeichnet die systematische und gezielte Beschaffung von frei verfügbaren Informationen, welche angereichert, ausgewertet und gebündelt werden.

Quellenoptimierung

Klassische Datengewinnung

Für die gesuchten Daten ist die Wahl der Tools essenziell in OSINT, da Suchmaschinen nur einen Teil des Internets abdecken und die Informationen nicht immer im benötigten Format vorliegen bietet es sich oftmals an Inhalte automatisiert zu crawlen und zu scrapen.

Vorteile:

- 24/7 automatisierte Datenerhebung
- Große Datenmengen in essenzielle Informationen

Nachteile:

- Erforderte den Seitenaufbau zu kennen
- Änderungen an der Quelle erforderten Nachkonfiguration

Klassische Datengewinnung

Hierfür mussten die Webelemente mit den Inhalten identifiziert werden. Anschließend mussten die relevanten Informationen extrahiert werden.

A Chinese Fentanyl Smuggling Network's Footprints in Japan

div.singular_content_text_content 725 × 9121.52

This article is the result of a collaboration with Japanese publishing partner Nikkei. You can find Nikkei's investigation [here](#).

Earlier this year, a man and a woman stood trial in a New York courtroom on charges related to the illicit drugs trade. They had been arrested as part of an undercover sting by the US Drug Enforcement Administration (DEA) after more than 200 kilograms of precursor chemicals used to make the synthetic opioid fentanyl were shipped from China to the US. It was enough to make 25 million deadly doses of the drug, authorities said.

The Chinese nationals were also accused of conspiring to import tonne-quantities of fentanyl precursors to the US, where tens of thousands of people die from opioid

```
<html class="no-js" lang="en-GB">
  <!--[endif]-->
  <head>
  </head>
  <body class="post-template-default single single-post postid-49509 single-r" itemscope itemtype="//schema.org/WebPage">
    <header class="site_header">
    </header>
    <div class="site_header--search d--f fd--r ai--c">
    </div>
    <div class="mobile-menu">
    </div>
    <script>
    </script>
    <main class="site_content">
      <div class="singular">
        <div class="container">
          <div class="singular_content">
            <aside class="singular_content_aside">
            </aside>
            <div class="singular_content_text">
              <div class="singular_content_text_title">
              </div>
              <div class="singular_content_text_meta">
              </div>
              <div class="singular_content_text_content">
                <p>
                </p>
                <p>
                </p>
                <p>
                </p>
                <div class="wp-block-image">
                </div>
                <p>
                </p>
                <p>
                </p>
                <p>
                </p>
                <p>
                </p>
                <div class="wp-block-image">
                </div>
              </div>
            </div>
          </div>
        </div>
      </div>
    </main>
  </body>
</html>
```

KI gestützte Datengewinnung

Wird das Crawling mit einer LLM verknüpft, müssen die Daten nicht im Quelltext identifiziert werden, sondern können per Prompt aus den Rohdaten extrahiert werden.

Vorteile:

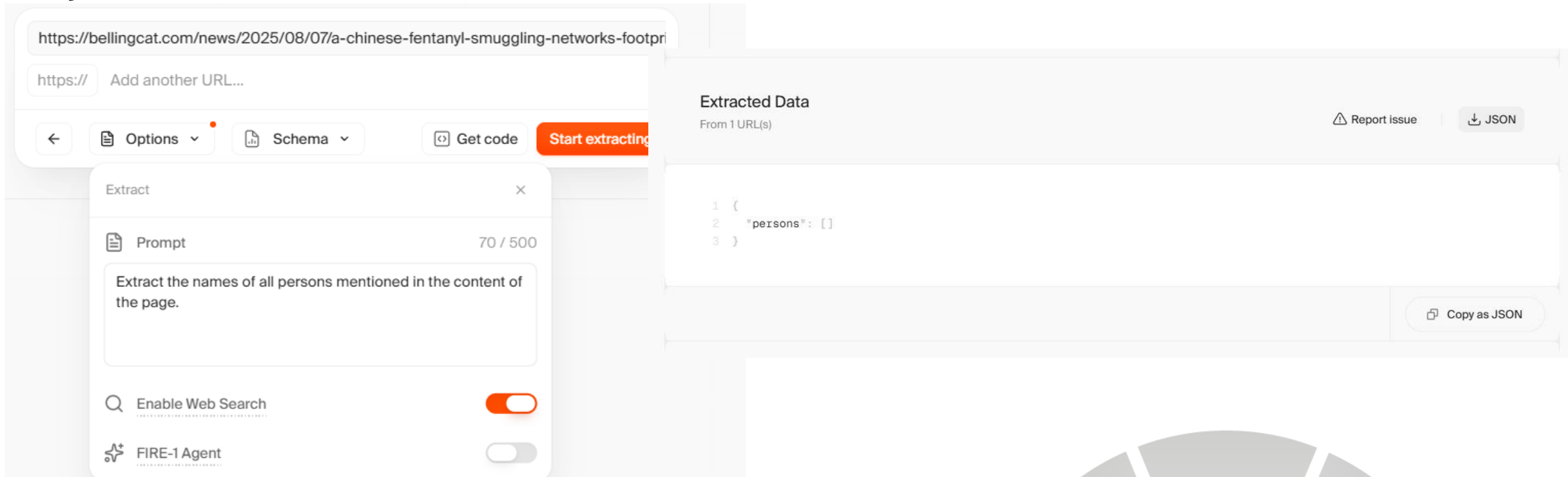
- 24/7 automatisierte Datenerhebung
- Große Datenmengen in essenzielle Informationen
- Flexible für diverse Quellen einsetzbar
- Keine Nachkonfiguration

Nachteile:

- Die Präzision der Daten kann schwanken
- Die benötigte Rechenleistung oder die Kosten steigen mit Quellenanzahl exponentiell

KI gestützte Datengewinnung

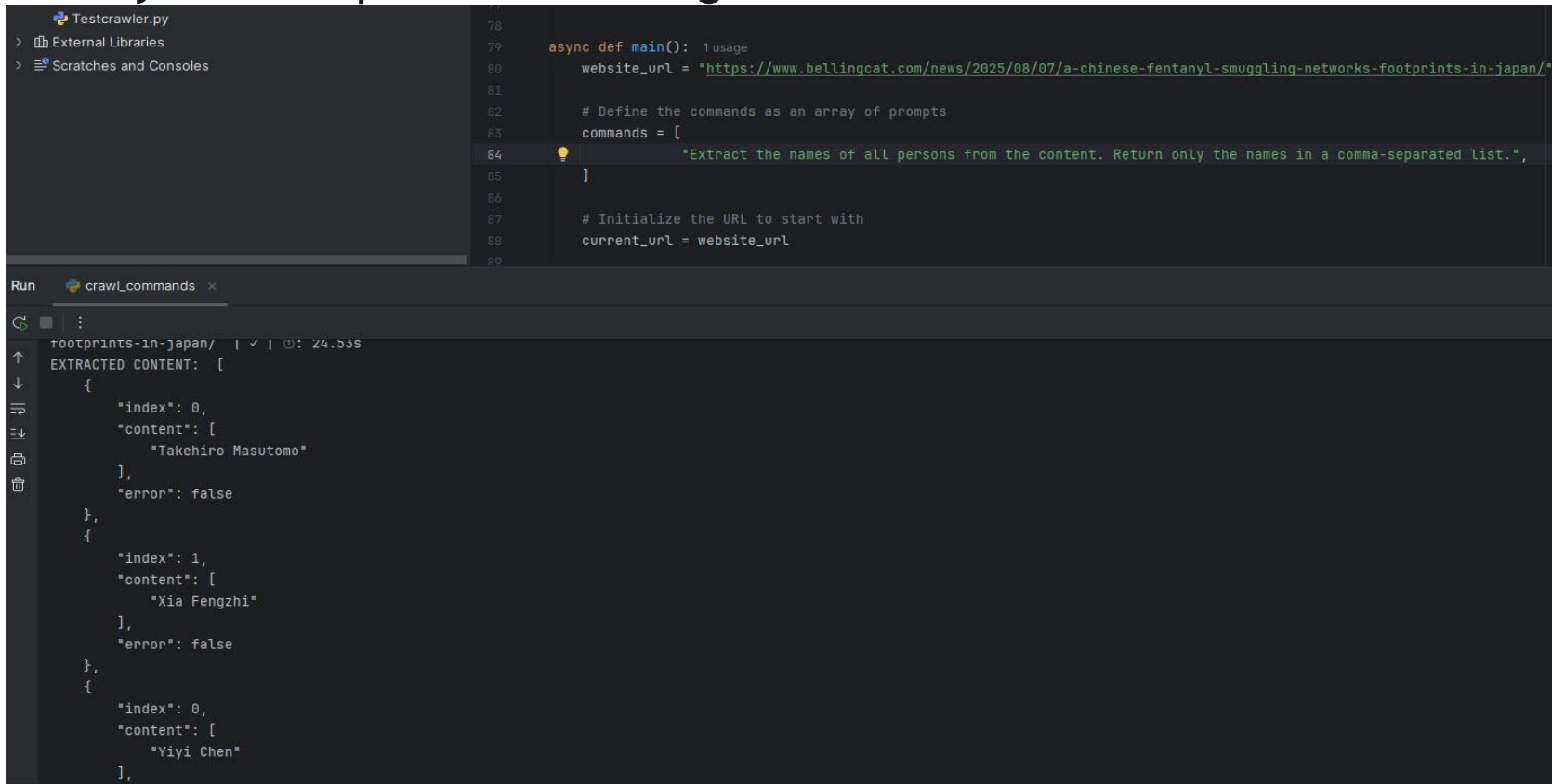
Für diese Art der Datenerhebung gibt es kostenpflichtige Webtools oder open source Projekte.



Firecrawl kostenloser Playground

KI gestützte Datengewinnung

Ein Python Skript in Verbindung mit einer Ollama lokalen KI zum Scrapen mit LLM.



The screenshot shows a code editor with a file named 'Testcrawler.py'. The script is an asynchronous Python function 'main()' that scrapes a website and uses an LLM to extract names. The website URL is 'https://www.bellingcat.com/news/2025/08/07/a-chinese-fentanyl-smuggling-networks-footprints-in-japan/'. The prompt instructs the LLM to 'Extract the names of all persons from the content. Return only the names in a comma-separated list.' The output, shown in the 'Run' panel, is a JSON array of three objects, each containing an index, a list of names, and a boolean error flag. The names extracted are 'Takehiro Masutomo', 'Xia Fengzhi', and 'Yiyi Chen'.

```
78
79 async def main(): 1 usage
80     website_url = "https://www.bellingcat.com/news/2025/08/07/a-chinese-fentanyl-smuggling-networks-footprints-in-japan/"
81
82     # Define the commands as an array of prompts
83     commands = [
84         "Extract the names of all persons from the content. Return only the names in a comma-separated list.",
85     ]
86
87     # Initialize the URL to start with
88     current_url = website_url
89
```

Run crawl_commands x

rootprints-in-japan/ | ✓ | ⌚: 24.53s

EXTRACTED CONTENT: [

```
{
  "index": 0,
  "content": [
    "Takehiro Masutomo"
  ],
  "error": false
},
{
  "index": 1,
  "content": [
    "Xia Fengzhi"
  ],
  "error": false
},
{
  "index": 0,
  "content": [
    "Yiyi Chen"
  ],
  "error": false
},
]
```

Crawl4ai + Ollama mit Deepseek R1 14b

KI gestützte Datengewinnung

Taranis AI als KI gestütztes OSINT Tool zum Monitoren und Analysieren von Datenfeeds oder Webscrapes.

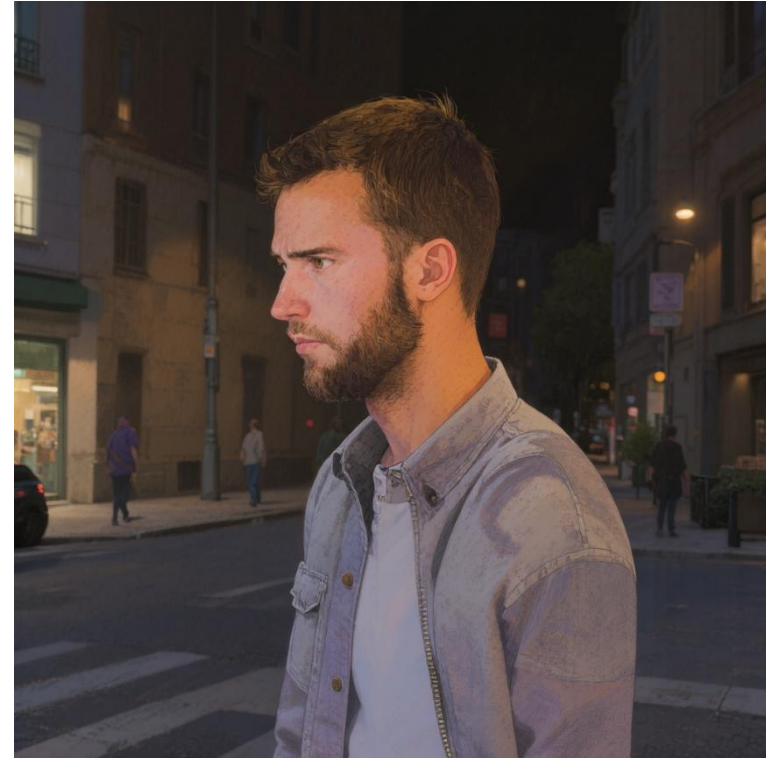
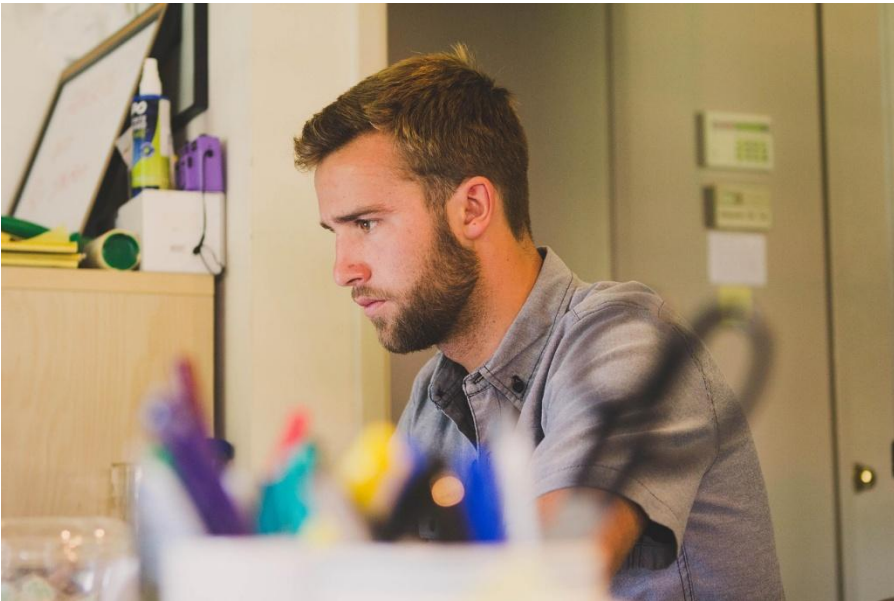
The screenshot displays the Taranis AI web interface. The top navigation bar includes links for Administration, Dashboard, Assess, Analyze, Publish, and Assets. The main content area shows a list of articles, each with a title, publication date, tags, and a brief description. The sidebar on the left contains a search bar, a dropdown for items per page (set to 100), and filter options for Source, Filter, and Tags. The articles listed include:

- Tageszusammenfassung - 26.09.2025**: End-of-Day report Timeframe: Donnerstag 25-09-2025 18:00 - Freitag 26-09-2025 18:00. Handler: Guenes Holler Co-Handler: Felician Fuchs. News: Schwerwiegende Sicherheitslücken in Cisco Adaptive Security Appliance - aktiv ausgenutzt - Updates verfügbar. Cisco hat Informationen zu einer vermutlich bereits seit einigen Monaten laufenden Angriffskampagne veröffentlicht. Im Rahmen dieser Kampagne haben Angreifer:innen, denen bereits im vergangenen Jahr eine breitgefächerte Kampagne gegen Edge-Devices zugerechnet wurde, Cisco Adaptive Security Appliance (ASA) Systeme der 5500-X Reihe welche "VPN web service..."
- Schwerwiegende Sicherheitslücken in Cisco Adaptive Security Appliance - aktiv ausgenutzt - Updates verfügbar**: 26. September 2025 Beschreibung Cisco hat Informationen zu einer vermutlich bereits seit einigen Monaten laufenden Angriffskampagne veröffentlicht. Im Rahmen dieser Kampagne haben Angreifer:innen, denen bereits im vergangenen Jahr eine breitgefächerte Kampagne gegen Edge-Devices zugerechnet wurde, Cisco Adaptive Security Appliance (ASA) Systeme der 5500-X Reihe welche "VPN web services" kompromittiert um in weiterer Folge auf den übernommenen Geräten Schadsoftware zu platzieren und Daten zu stehlen. Aufgrund der Natur der Angriffe und der mutmaßlich verantwortlichen Täter:innen ist nach aktuelle...
- Tageszusammenfassung - 24.09.2025**: End-of-Day report Timeframe: Dienstag 23-09-2025 18:00 - Mittwoch 24-09-2025 18:00. Handler: Michael Schlagenhauser Co-Handler: n/a. News: Supermicro server motherboards can be infected with unremovable malware. One of the two vulnerabilities is the result of an incomplete patch. Supermicro released in January, said Alex Matrosov, founder and CEO of Binary, the security firm that discovered it. [...] The two new vulnerabilities tracked as CVE-2025-7937 and CVE-2025-6198 reside inside silicon soldered onto Supermicro motherboards that run servers inside data centers. [...] Supermicro said it has updated the BMC firmware to mitigate the...
- Crashing BIRD 3 by sending a Notification (CVE-2025-59688)**: Over July and August, we received several reports about always the same cryptic bug happening quite sparsely. We were methodically disproving every hypothesis about this bug and slowly accepting our feat of creating a very specific and complex test setup to reproduce and properly analyze the bug. Last week (and the weekend before), this changed significantly. Over just 48 hours we received more crash reports than in the last two months. Yet, expecting that most of these are going to be the same bug over and over again, we calmly opened them one after another to find out that ... we have never seen any single one of these. One...
- Tageszusammenfassung - 23.09.2025**: End-of-Day report Timeframe: Montag 22-09-2025 18:00 - Dienstag 23-09-2025 18:00. Handler: Michael Schlagenhauser Co-Handler: n/a. News: SonicWall releases SMA100 firmware update to wipe rootkit malware. SonicWall has released a firmware update that can help customers remove rootkit malware deployed in attacks targeting SMA 100 series devices. https://www.bleepingcomputer.com/news/security/sonicwall-releases-sma100-firmware-update-to-wipe-rootkit-malware/ GitHub Mandates 2FA and Short-Lived Tokens to Strengthen npm Supply Chain Security. GitHub on Monday announced that it will be changing its authentication...

Smarte Analyse

Bildgeneratoren

Bildanalysen sind in OSINT ein elementarer Bestandteil, KI erschwert zunehmend den Wahrheitsgehalt eines Bildes zu bestimmen. Gleichzeitig war es nie so einfach passende Avatare für Aliase zu erstellen.



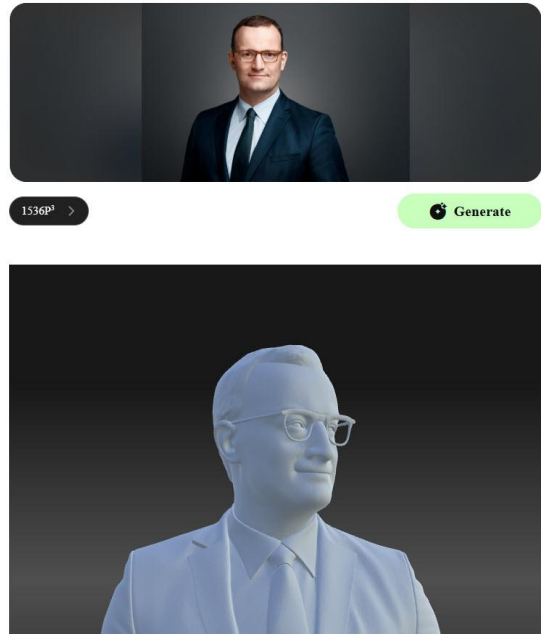
Bildgeneratoren

Auch das beibehalten des (komplett) generierten Modells bei weiteren Bildern oder eine leichte Modifikation davon ist möglich.



Daten analysieren & anreichern

Bei der Gesichtserkennung und Suchmaschinen für diese gibt es durch KI gewaltige Fortschritte. War die Wahl eines passenden Bildes früher entscheidend für die Qualität der Ergebnisse, so können jetzt kostenlose 3D-Modelle erzeugt werden um verschiedene Winkel zu testen.



3D-Bild aus einem Foto durch
Sparc3D-KI

Daten analysieren & anreichern

Bei der Gesichtserkennung oder dem Rekonstruieren von Gesichtern ergeben sich somit neue Möglichkeiten und Ansätze.



1536p >

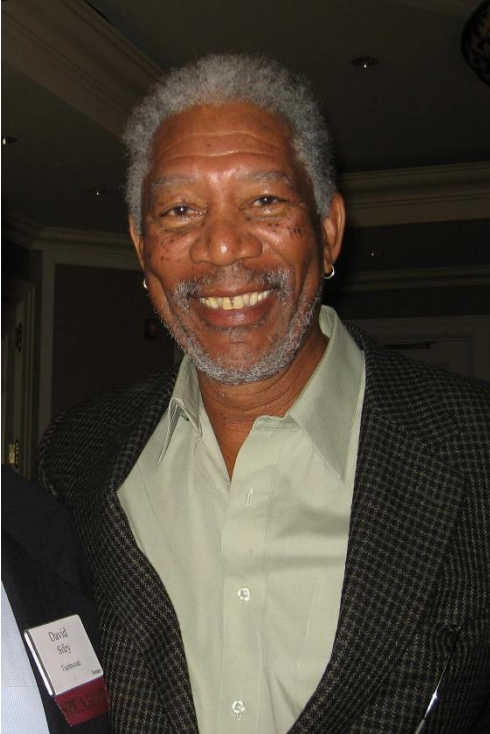
 Generate



3D-Bild aus einem Foto durch
Sparc3D-KI

Daten analysieren & anreichern

Bei Foto-Upscaling KIs muss jedoch berücksichtigt werden, dass diese Bilder verfälschen.



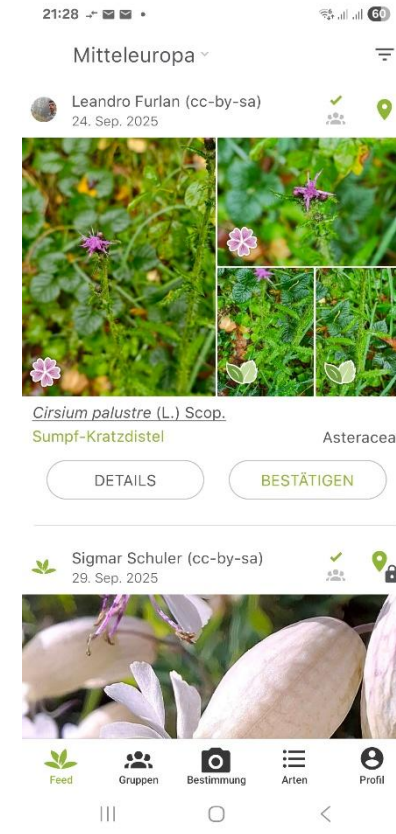
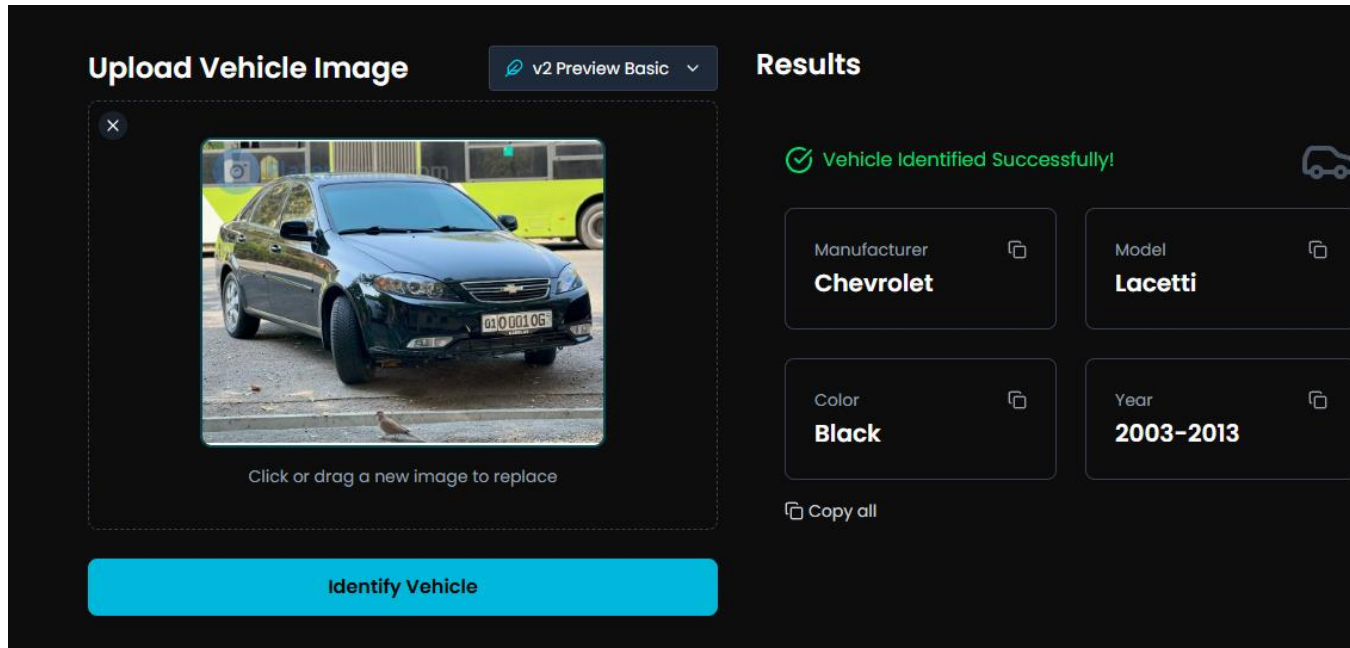
Daten analysieren & anreichern

Bei Foto-Upscaling KIs muss jedoch berücksichtigt werden, dass diese Bilder verfälschen.



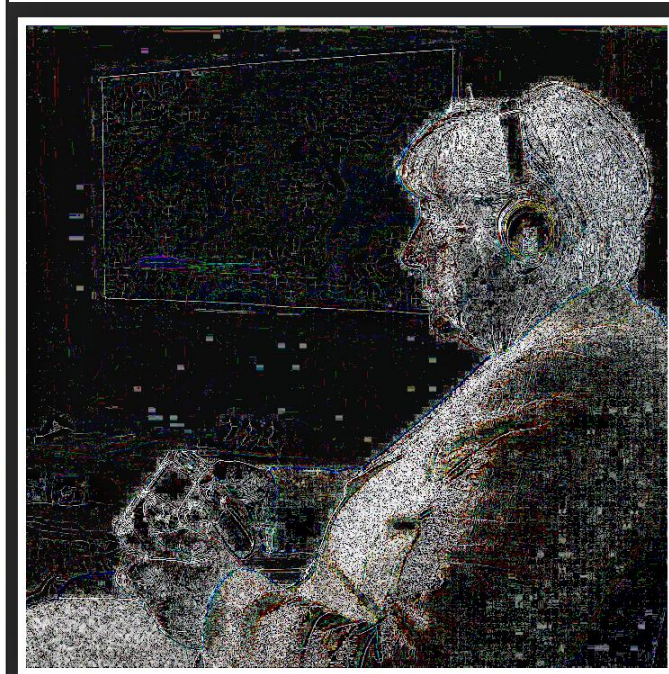
Daten analysieren & anreichern

Dedizierte Kls, welche auf Pflanzen oder Fahrzeuge trainiert wurden liefern meist präzise Ergebnisse.



Deepfakes

Bildmanipulationen werden durch den Einsatz von KI schwerer erkennbar, auch mit dedizierten Tools.



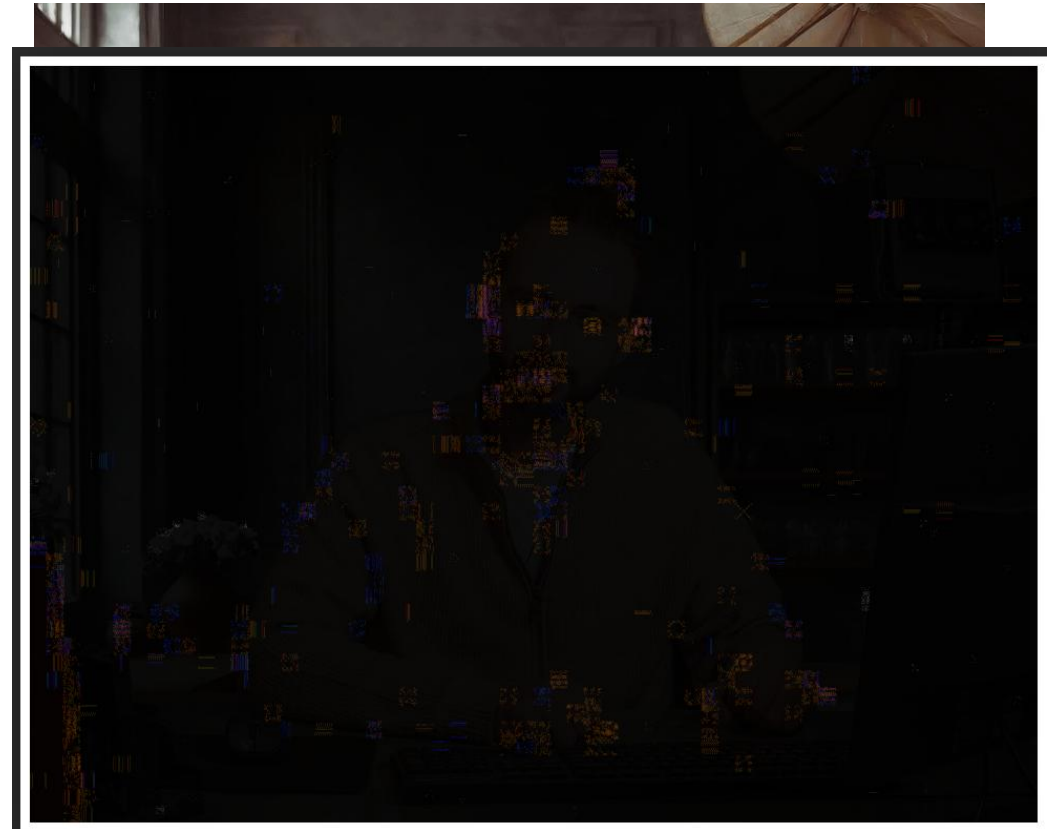
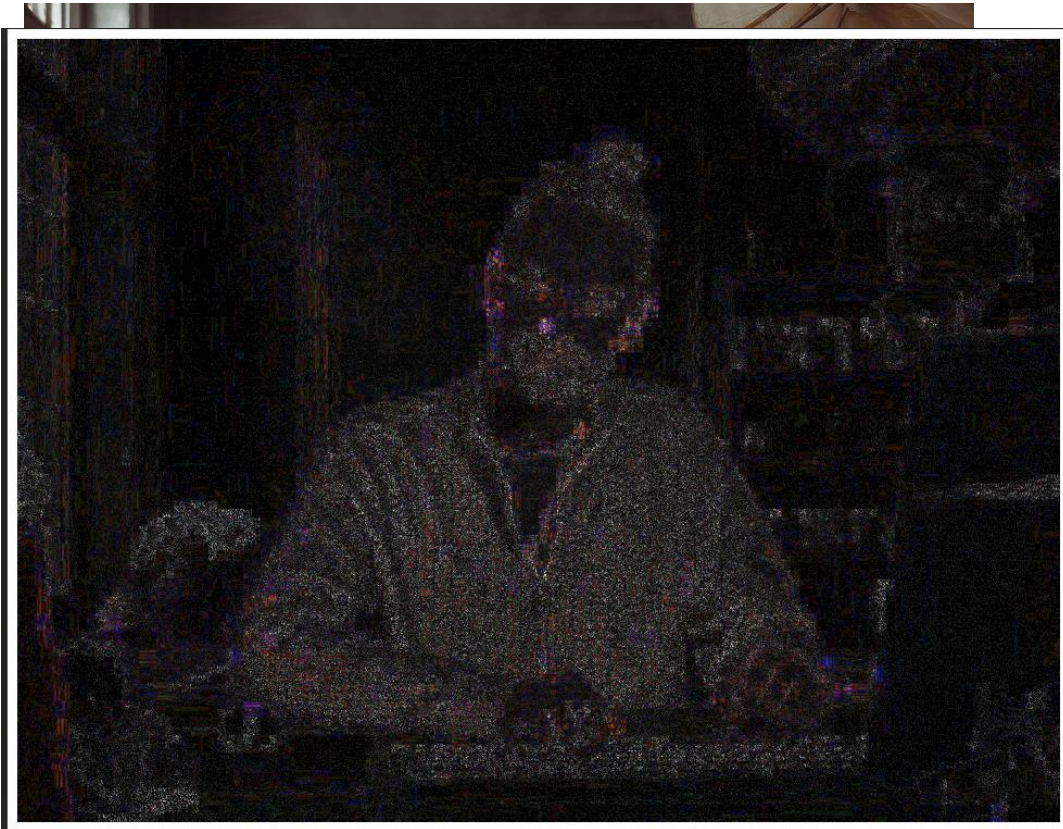
Deepfakes

Bildmanipulationen werden durch den Einsatz von KI schwerer erkennbar, auch mit dedizierten Tools.



Deepfakes

Bildmanipulationen werden durch den Einsatz von KI schwerer erkennbar, auch mit dedizierten Tools.



Geo-Analyse mit LLMs

Standorte sind in OSINT meist von hohem Interesse und Datenwert. Diese Informationen können unter anderem aus visuellen Inhalten gewonnen werden.



Wo wurde dieses Foto aufgenommen?

Das Foto wurde sehr wahrscheinlich in einer deutschen Stadt aufgenommen. Es gibt mehrere Hinweise darauf:

1. **Ladenschilder:** Das Schild von "Nordsee" (eine bekannte deutsche Fischrestaurantkette) ist deutlich sichtbar. Auch das "O2"-Logo (ein Mobilfunkanbieter, der in Deutschland sehr verbreitet ist) ist vorhanden.
2. **Architektur:** Die Architektur der Gebäude – insbesondere die Mischung aus älteren, schmalen Häusern und modernen Fassaden – ist typisch für deutsche Fußgängerzonen.
3. **Sprache:** Die sichtbaren Wörter (z. B. „Passage“) sind auf Deutsch.
4. **Straßenbild:** Die Straßenmöblierung, Pflasterung und das Design der Fußgängerzone passen sehr gut zu typischen deutschen Innenstädten.



Die Stadt lässt sich aus diesem Foto allein nicht mit absoluter Sicherheit bestimmen, aber basierend auf dem

Ich habe recherchiert und hier sind meine Erkenntnisse:

Was ich gefunden habe:

- Die Nordsee-Filiale in Oldenburg ist unter der Adresse **Schloßplatz 3, 26122 Oldenburg** gelistet. nordsee.com +1
- Der O₂-Shop befindet sich ebenfalls an **Schloßplatz 3, 26122 Oldenburg**. 11880 Branchen... +2
- In den Angaben zu den Schlosshöfen („Schlosshöfe Oldenburg“) ist als Adresse ebenfalls **Schloßplatz 3** angegeben, was darauf hindeutet, dass es sich bei dieser Stelle um ein Einkaufs- oder Geschäftszentrum handelt. Schlosshöfe Old... +1
- Ein Ladenverzeichnis des Einkaufszentrums „Schlosshöfe Oldenburg“ nennt unter den Mietern **Nordsee** und **O2** zusammen in der Adresse **Schloßplatz 3**. Shopunits



Vergleich mit dem Foto & Schlussfolgerung:

- Wenn beide Geschäfte dieselbe Adresse haben, dann müssten sie nebeneinander oder sehr nahe beieinander sein — das passt gut zu dem Foto, in dem „Nordsee“ und „O₂“ an nebeneinanderliegenden Fassaden sichtbar sind.

Geo-Analyse mit LLMs

Standorte sind in OSINT meist von hohem Interesse und Datenwert. Diese Informationen können unter anderem aus visuellen Inhalten gewonnen werden.

Hier sind ein paar Informationen, wo Shops nahe beieinander liegen:

Wiesbaden

Geschäft

Nordsee

O2 Shop

Abstand der Hausnummern:
Kirchgasse 46 (Nordsee) vs. Kirchgasse 47 (O2 Shop) im Sinne von nebenan.

Städte mit O ₂ -Shop + Nordsee im Nahbereich (< 5 Hausnummern)				
Stadt	O ₂ -Shop (Adresse)	Nordsee (Adresse)	Abstand (ca.)	Bemerkungen
Berlin – Mitte	Otto-Brenner-Platz 1, 10178 Berlin	Nordsee, Friedrichstraße 79, 10117 Berlin	ca. 3 Hausnummern (gleiche Straße, unterschiedliche Hausnummernbereiche)	Beide liegen im belebten Shopping- und Büroviertel nahe dem Hauptbahnhof.
Hamburg – St. Pauli	O ₂ -Shop, Reeperbahn 21, 20359 Hamburg	Nordsee, Reeperbahn 29, 20359 Hamburg	ca. 4 Hausnummern (gleiche Straße)	Direkt am „Kiez“; kurzer Fußweg über die Straße hinweg.
München – Innenstadt	O ₂ -Shop, Kaufingerstraße 3, 80331 München	Nordsee, Kaufmannshof 2, 80331 München	< 5 Hausnummern (benachbarte Gebäude)	Im Herzen der Münchner Altstadt, nahe dem Marienplatz.
Köln – Innenstadt	O ₂ -Shop, Hohe Straße 1, 50667 Köln	Nordsee, Hohe Straße 9, 50667 Köln	ca. 4 Hausnummern (gleiches Straßennetz)	Direkt am Kölner Dom und dem Shopping-Mittelpunkt.
Düsseldorf – Altstadt	O ₂ -Shop, Schadowstraße 5, 40212 Düsseldorf	Nordsee, Schadowstraße 13, 40212 Düsseldorf	ca. 3 Hausnummern (gleiche Straße)	In der Fußgängerzone nahe dem Hauptbahnhof.
Stuttgart – Zentrum	O ₂ -Shop, Königstraße 16, 70173 Stuttgart	Nordsee, Königstraße 22, 70173 Stuttgart	< 5 Hausnummern (kurzer Seitenweg)	Im Stuttgarter Shopping-Kern nahe dem Schlossplatz.
Leipzig – Innenstadt	O ₂ -Shop, Petersstraße 3, 04109 Leipzig	Nordsee, Petersstraße 9, 04109 Leipzig	ca. 4 Hausnummern (gleiches Straßennetz)	Beide Filialen liegen im historischen Zentrum nahe dem Augustusplatz.
Frankfurt am Main – Innenstadt	O ₂ -Shop, Zeil 2, 60313 Frankfurt	Nordsee, Zeil 8, 60313 Frankfurt	< 5 Hausnummern (gleiche Straße)	Im größten Einkaufsboulevard Frankfurts, kurzer Fußweg über die Straße.
Dresden –	O ₂ -Shop, Prager Str. 1,	Nordsee, Prager Str. 7,	ca. 4 Hausnummern (gleiche Straße)	Direkt am Altmarkt, nahe dem

in O₂-Shop nicht mit genau einer Hausnummer

Wiesbaden. [nordsee.com](#) +2

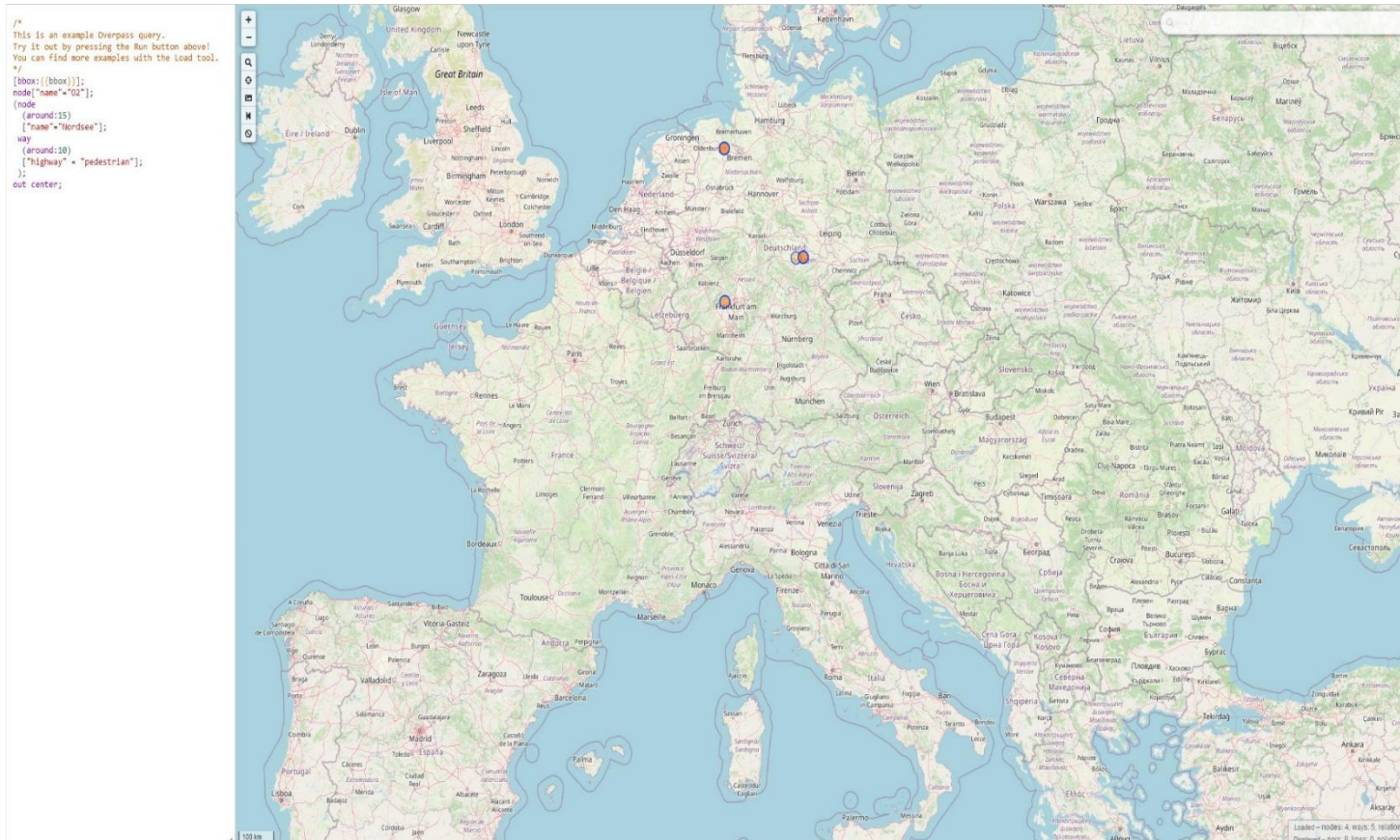
3 Wiesbaden. [globuya.com](#) +2

2-4 Hausnummern.

den einen Fall gibt, wo die beiden genau eine ?

Geo-Analyse mit LLMs

Standorte sind in OSINT meist von hohem Interesse und Datenwert. Diese Informationen können unter anderem aus visuellen Inhalten gewonnen werden.



HERZLICHEN DANK

für Ihre Teilnahme

Janis Kinast



Spurensuche 2.0:

Wie Künstliche Intelligenz OSINT-
Operationen transformiert



Exkl. Rabatt 350€
qs350BIHK

SC350

Open Source Intelligence (OSINT) Basics



SC355

Open Source Intelligence (OSINT) Practitioner



Herzlichen Dank
FÜR IHRE TEILNAHME



Wir setzen auf **Qualität**.
Setzen Sie sich zu uns.

qSkills GmbH & Co. KG

Südwestpark 65
90449 Nürnberg

Telefon: +49 (911) 80 10 3-0
Fax: +49 (911) 80 10 3-39
E-Mail: info@qskills.de

Folgen Sie uns auf:



Zur Website:



www.qskills.de

Bildquelle: iStock.com/Ridofranz

