

Hands-on: Metadatenanalyse

Motivation: Die Schattenseite der Metadaten

Stell dir vor, du postest ein Foto von deinem süßen Kätzchen – gemütlich auf der Couch, im Hintergrund Bücherregal und Pflanzen. Total harmlos, oder?

Falsch.

Denn wenn du dieses Bild mit deinem Smartphone aufnimmst und auf Plattformen wie **flickr** hochlädst, landen im Netz nicht nur deine vier Wände – sondern oft auch deine exakten **GPS-Koordinaten**. Viele professionelle Fotoplattformen – darunter auch **flickr** – entfernen diese Metadaten **nicht automatisch**.

Warum? Ganz einfach: Weil die Plattformen davon ausgehen, dass ihre Nutzer wissen, was sie tun. In der Fotografie-Szene gilt es oft sogar als Feature, dass Metadaten wie Kameraeinstellungen oder Aufnahmeorte erhalten bleiben – als digitaler Fingerabdruck für Stil, Ort und Technik. Wer ein Bild bewusst mit Standort teilen will, kann das so auch tun.

Aber was passiert, wenn einem diese Metadaten gar nicht bewusst sind?

Metadaten sind kein Spaß... but now it's doxing time!

Was ihr lernen werdet

- Wie man EXIF-Daten ausliest,
- Wie man GPS-Koordinaten in Dezimalgrad umrechnet,
- Wie man Standorte auf Karten anzeigt,
- Und – ganz wichtig – wie man sich vor unerwünschter Weitergabe von Metadaten schützt!

1. Vorbereitung: Bilder entpacken

Im Workshop-Repository liegt eine ZIP-Datei mit Bildern. Diese müsst ihr über das Terminal entpacken. Anschließend wechselt ihr in den Zielordner:

```
mkdir -p ~/Desktop/Bilder

cd /home/workshop/IT-Workshop/Hands-on

unzip bilderstrippen.zip -d ~/Desktop/Bilder

cd ~/Desktop/Bilder/<Deine Gruppe>
```

2. EXIF-Daten auslesen

EXIF-Daten (Exchangeable Image File Format) sind die Informationen, die von digitalen Kameras oder Smartphones zusammen mit einem Foto gespeichert werden. Dazu gehören viele nützliche Informationen, wie zum Beispiel:

- Kameramodell
- Datum und Uhrzeit der Aufnahme
- GPS-Position (falls aktiviert)

Mit `exiftool` könnt ihr diese Daten einfach auslesen und auch manipulieren. Gebt folgenden Befehl im Terminal ein:

```
exiftool foto1.jpg
```

Sucht nach den GPS-Daten:

```
GPS Latitude   : 48 deg 12' 34.56" N
GPS Longitude  : 16 deg 22' 11.11" E
```

3. Was sind Längen- und Breitengrade?

Die GPS-Position eines Punktes auf der Erde wird über zwei Werte angegeben:

- **Breitengrad (Latitude)**: Die Nord-Süd-Ausrichtung (vom Äquator aus).
- **Längengrad (Longitude)**: Die Ost-West-Ausrichtung (vom Nullmeridian aus, auch **Greenwich** genannt).

Umrechnung in Dezimalgrad

Die Umrechnung von Grad, Minuten und Sekunden in Dezimalgrad erfolgt nach folgender Formel:

$$\text{Dezimalgrad} = \text{Grad} + \frac{\text{Minuten}}{60} + \frac{\text{Sekunden}}{3600}$$

Beispiel für den Breitengrad (Latitude):

$$48^{\circ}12'34.56'' \text{ N} = 48 + \frac{12}{60} + \frac{34.56}{3600} = 48.2096^{\circ} \text{ N}$$

Beispiel für den Längengrad (Longitude):

$$16^{\circ}22'11.11'' \text{ E} = 16 + \frac{22}{60} + \frac{11.11}{3600} = 16.3698^{\circ} \text{ E}$$

Achtet auch auf die Himmelsrichtungen:

- N und E bleiben positiv
- S und W werden negativ

Die Dezimalwerte (48.2096 für den Breitengrad und 16.3698 für den Längengrad) können nun verwendet werden, um den Standort auf einer Karte anzuzeigen.

Standort auf Karte anzeigen

Nun, da ihr die Dezimalwerte für die GPS-Koordinaten habt, geht zur [OpenStreetMap](#)-Webseite und gebt die Koordinaten einfach in das **Suchfeld** ein. Gebt den **Breitengrad** und den **Längengrad** mit einem Komma getrennt ein, zum Beispiel:

48.2096, 16.3698

4. Challenge: Metadaten entfernen!

Jetzt seid ihr dran – die **Metadaten eines Bildes sollen vollständig gelöscht** werden.

Regeln:

- Es gibt **keine Hilfe** von uns!
- Ihr dürft [duck.ai](#) befragen.
- Zeigt uns das Originalbild und das bereinigte Bild.

Bitte tragt eure Daten nach erfolgreicher Auswertung in das Formular unten ein:

1. Wählt eure Gruppe aus:

2. Tragt eure ermittelten Dezimal-Koordinaten ein (z.B. 48.2096, 16.3698):

3. Tragt hier die ermittelte Adresse ein

Disclaimer

Dieses Hands-on zeigt reale Beispiele aus dem Internet – und ja, die betroffenen Personen haben diese Fotos tatsächlich selbst, unter Klarnamen und inklusive Metadaten, öffentlich gemacht.

Wir „doxen“ hier niemanden – das haben die Leute schon selbst erledigt. Unser Ziel ist es, euch zu zeigen, wie schnell so etwas passieren kann – und warum es wichtig ist, zu wissen, was man da eigentlich ins Netz stellt.

Auch wenn das Ganze ein bisschen wie Hacker-CSI wirkt: *Nutzt euer neues Wissen mit Verstand – und nicht, um euren Nachbarn zu stalken.*

Denn: **Metadaten sind wie Glitzer – einmal verteilt, bekommst du sie nie wieder los.**

Have fun – it's doxing time!