OSINT: Ich weiß wo dein Haus wohnt

jomo

Was ist OSINT?

- **O**pen **S**ource **Int**elligence
- Hat nichts mit quelloffener Software zu tun
- Informationsgewinnung aus öffentlichen Quellen (open source)
- Begriff von US-Geheimdiensten
- Zusammentragen von Details
- "Digitialer Fußabdruck"

Warum OSINT?

- Überprüfen von Informationen
  - Vertraue niemand!
  - Wichtig für Journalisten
- Weitere Informationen bekommen
  - Wichtig für Geheimdienste, Ermittlungsbehörden, Journalisten
  - Für Wissenshungrige

Warum OSINT?

- Leute im Internet stalken
  - Kenne die Methoden deiner Feinde
- Man entwickelt starkes Google-fu

OSINT vs. OPSEC

jack
@scobesx

had to delete my previous “NFTs are cringe” tweet, a monkey smoking a blunt in a top hat just dmed me a picture of my house on google maps

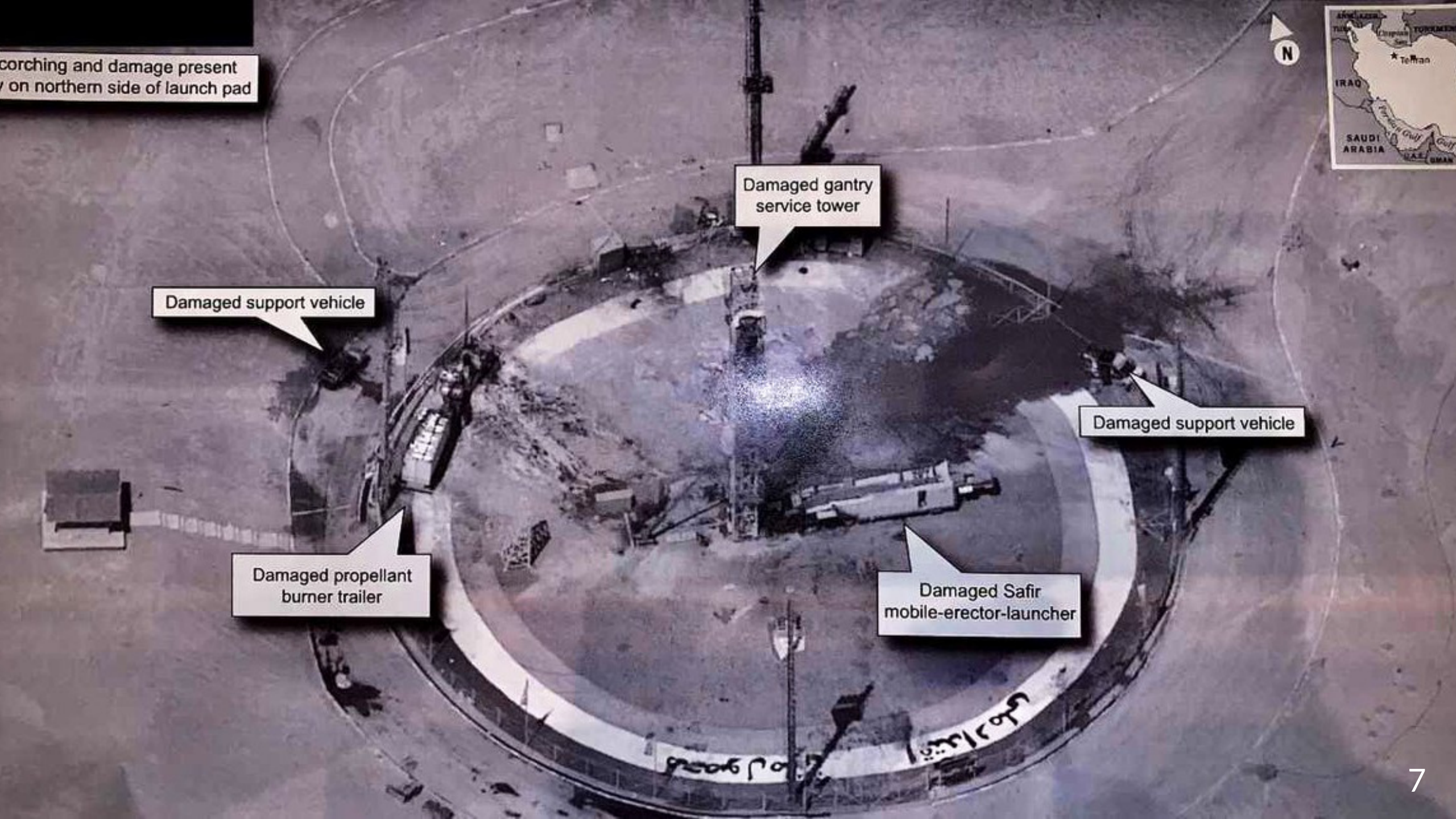
1:11 AM · Dec 14, 2021 · Twitter for iPhone

15.5K Retweets **476** Quote Tweets **210.4K** Likes

OPSEC?

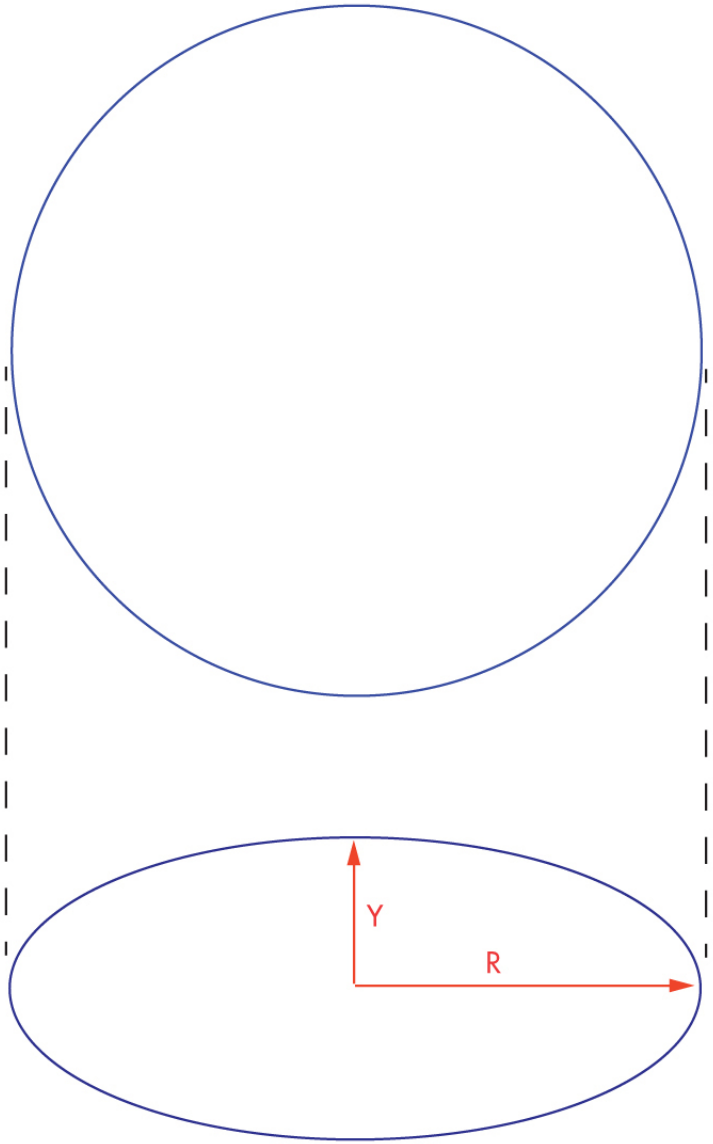
- **Op**erational **Sec**urity
  - Maßnahmen, um die Informationsgewinnung des Feindes einzuschränken
- Im Internet:
  - Datenschutz und Privatsphäre gewährleisten
  - Stalkern durch Datensparsamkeit Steine in den Weg legen

→ "OpSec für Datenreisende" von ths & linus @ 35c3


corching and damage present
on northern side of launch pad
N
Tehran
IRAQ
SAUDI ARABIA
Damaged gantry service tower
Damaged support vehicle
Damaged support vehicle
Damaged propellant burner trailer
Damaged Safir mobile-erector-launcher

Pibwl CC BY-SA 4.0

suncalc.org, Screenshot von @trbrtc

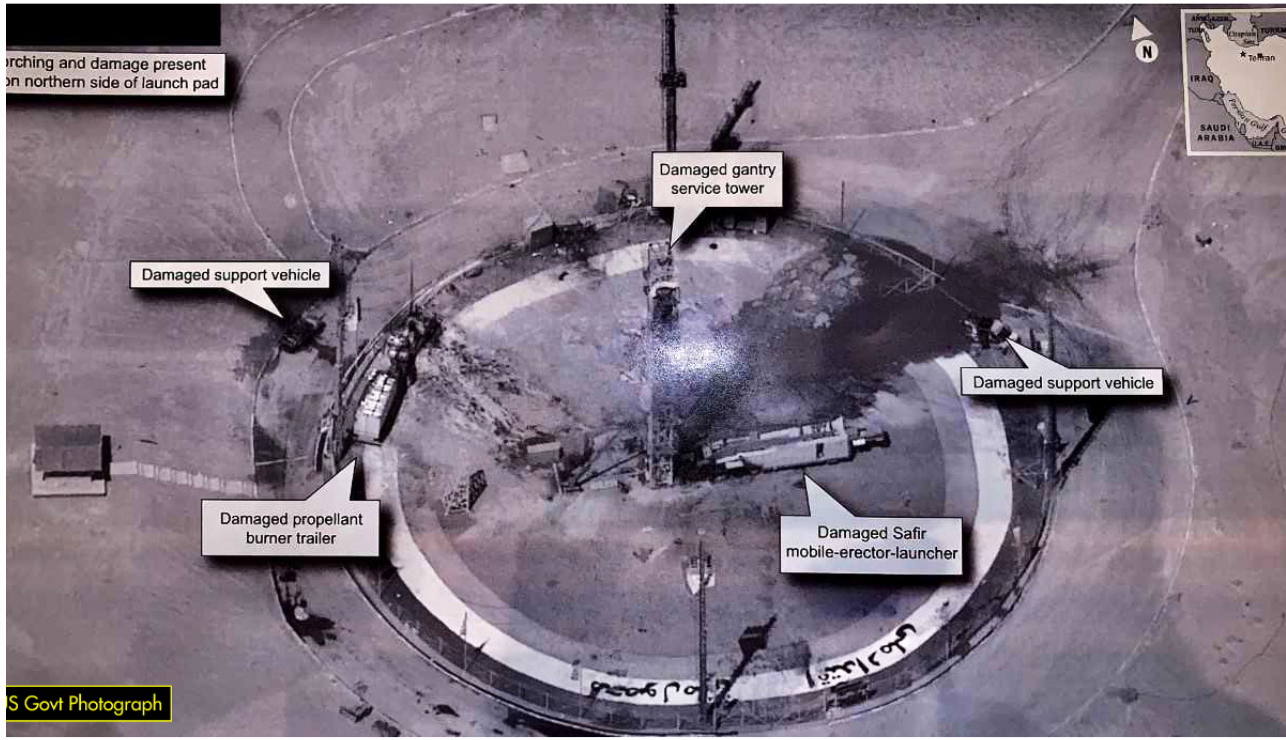


TOP VIEW

OBLIQUE VIEW

SIN α = Y/R

(α = view angle)



45
50
55
60
65
40
35
30
25
http://sattrackcam.blogspot.com
satellite ground track
09:43
Tehran
Imam Khomeini
Space Center
09:44
USA 224 position
at time of image
09:45
09:46

Geolokalisierung

Wo wurde das Foto gemacht?

- Details sammeln
- Recherchieren
- Ergebnis verifizieren

Details sammeln – Metadaten

- Exif & Co
- Datei- und Server-Metadaten (z.B. `Last-Modified`)
- Von wem stammt das Foto?

Details sammeln – Was ist zu sehen?

- Himmelsrichtung
- Schattenwurf
- Jahreszeit
- Umgebung (Berge, Meer, Flüsse, Wald, Urban, …)
- Geschäfte (Typ, Name, …)
- Fahrzeuge (Typ, Alter, Zustand, …)
- Menschen (Ethnie, Kleidung, …)
- Gebäude (Baustil, Höhe / Anzahl Etagen, Alter, Zustand, …)
- Straßenverkehr (Rechts-/Linksverkehr, Verkehrszeichen, …)

Recherche

- Einfach mal in Google schmeißen™
- Reverse-Bildersuche
- Wikipedia-Listen
- Datenbank-Webseiten
- Foto-Datenbanken

Reverse-Bildersuche

- Es gibt nicht nur Google Images!
- Google Lens
- Yandex
- Bing
- TinEye
- KarmaDecay
- Stock photos
- Logos / Trademarks

ubahnverleih CC BY-SA 4.0

Google

JPG ×

leisure

Alle | Bilder | Maps | Shopping | Mehr | Suchfilter

Ungefähr 3 Ergebnisse (0,78 Sekunden)

Bildgröße:
2048 × 1536

Keine anderen Größen für dieses Bild gefunden.

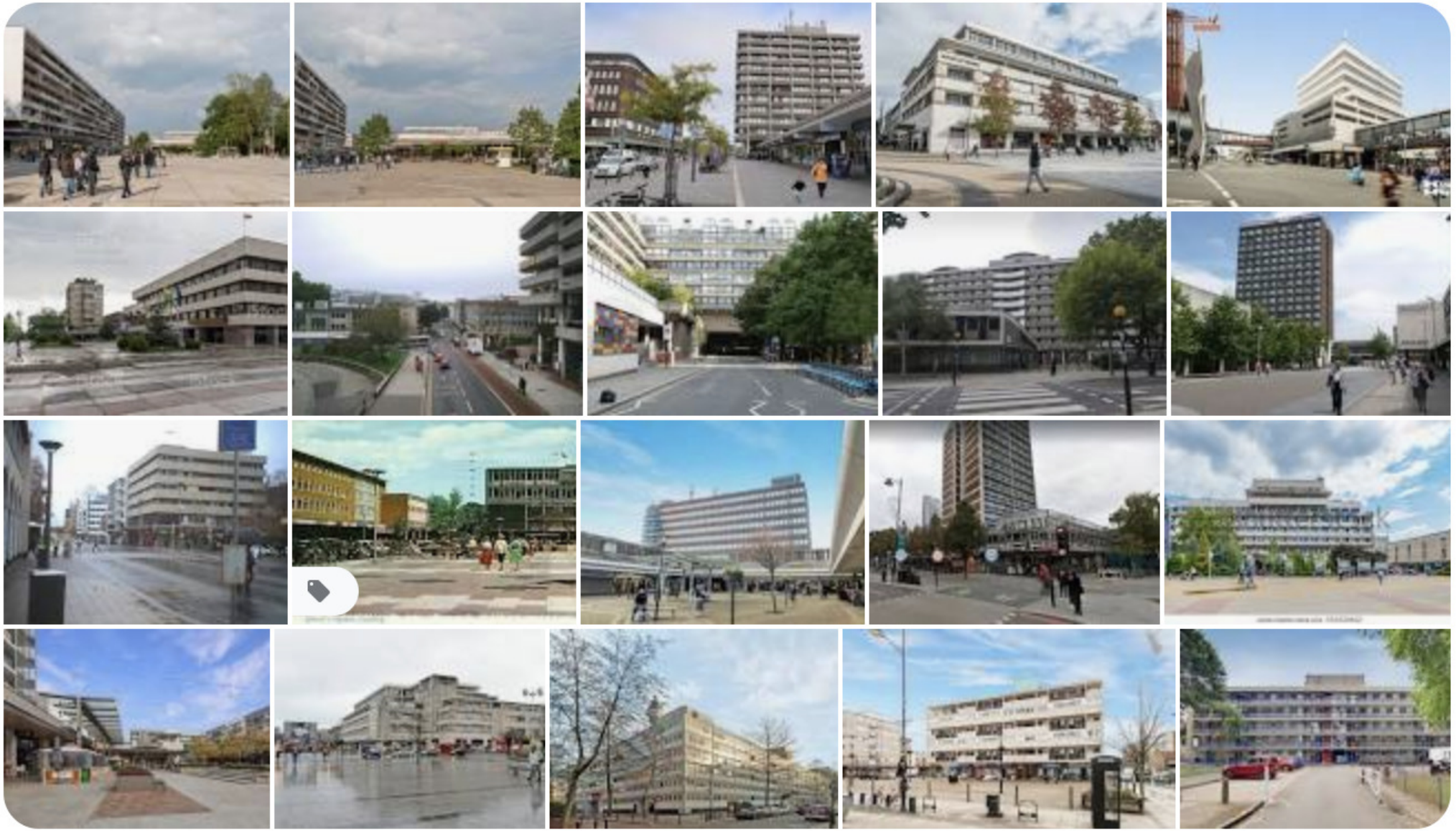
Mögliche verwandte Suchanfrage: ***leisure***

https://de.pons.com › übersetzung ▾ Diese Seite übersetzen

leisure - Englisch-Deutsch Übersetzung | PONS

Übersetzung Englisch-Deutsch für **leisure** im PONS Online-Wörterbuch nachschlagen! Gratis Vokabeltrainer, Verbtabellen, Aussprachefunktion.

Optisch ähnliche Bilder



Feedback geben

Microsoft Bing

All | Looks like | Tt Text | Related content

Looks like

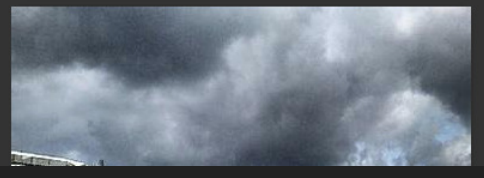
Congress Center Hamburg
Convention Center

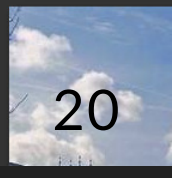
Tt Text

HAMBURG

Copy text | Search | Tt Enter Text Mode

Related content





Yandex

Uploaded image ×

Search

Web **Images** Video News Translate Disk Mail Ads

Original image size: 2048×1536

Select crop area

Other image sizes

No matching images found

Sites containing information about the image

Congress Center Hamburg (CCH) (Now Closed) - Convention Center in Hamburg

lv.foursquare.com

Photo taken at Congress Center Hamburg (CCH) by Bastian M. on 12/27/2012

Bildersuche Tipps & Tricks

- Bilder auf das zuschneiden, was man sucht
- Bilder bearbeiten, um das Gesuchte zu entzerren oder besser "sichtbar" zu machen

Yandex

Uploaded image ×

Search

Web **Images** Video News Translate Disk Mail Ads

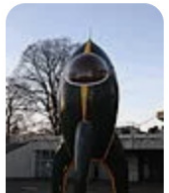
Original image size: 2048×1536

Cancel Done

Other image sizes

No matching images found

Sites containing information about the image



Category:Fairydust - Wikimedia Commons

commons.m.wikimedia.org

Media in category "Fairydust"

Image appears to contain

необычные скульптуры

современная скульптура

Similar images

Similar images

Original image size: 2048×1536

Cancel Done

Other image sizes

No matching images found

Sites containing information about the image

10+ Free Heinrich Hertz Tower & Hamburg Photos

pixabay.com

13 Free photos of Heinrich Hertz Tower

Image appears to co

телебашня гамбург

Similar images

Original image size: 2048×1536

Cancel Done

Other image sizes

No matching images found

Sites containing information about the image

File:Congress Center Hamburg CCH-CCC- (16119863935).jpg - Wikimedia Commons

commons.wikimedia.org

User:FlickreviewR.

Image appears t

вывеска лог

Similar images

Nichts ist wahr, alles ist erlaubt!

Yandex

Uploaded image ×

Search

Web **Images** Video Maps News Translate Q Services Music More

trm-design.mosantico.ru

Проекты разных лет

File:Congress Center Hamburg CCH-CCC- (16119863935).jpg - Wikimedia Commons

commons.wikimedia.org

User:FlickreviewR.

Wikimedi'Oc - Album de fòtos

wikimedioc.com

33C3 halfnarp: The talks that 'work for us' - CCC Event Blog

events.ccc.de

33C3 halfnarp: The talks that 'work for us'

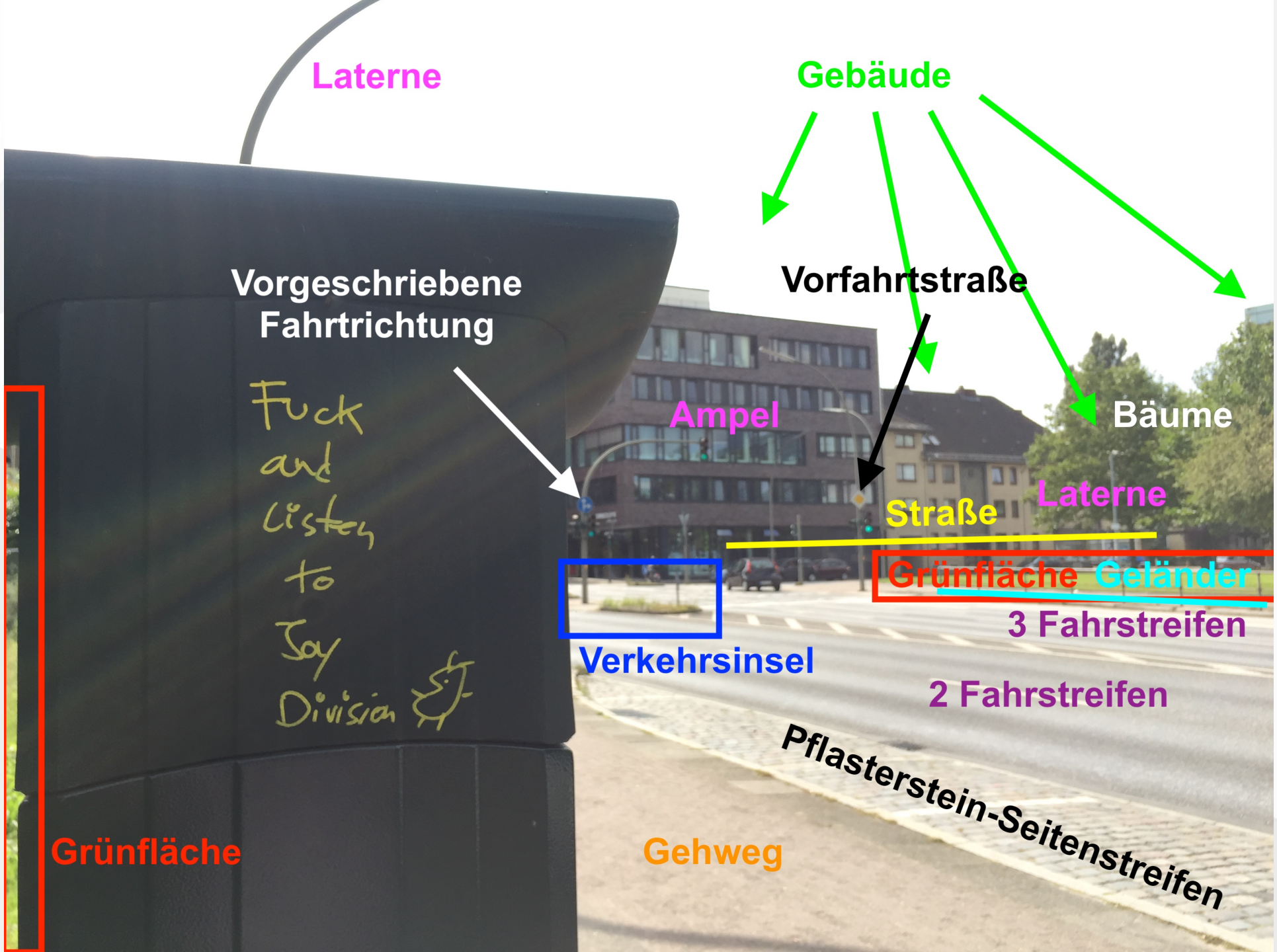
Listen und Datenbanken

- Gibt es für fast alles
  - Verbreitung von Planzen- oder Tierarten auf der Welt
  - Gebäude nach Baustil, Höhe, Baujahr, …
  - Flugdaten, Schiffdaten, Zugdaten, Satellitendaten, …
  - Flaggen, Verkehrszeichen, Kfz-Kennzeichen
  - Streetart
  - Wetterdaten
  - WLAN-Netzwerke
  - Geleakte Passwörter

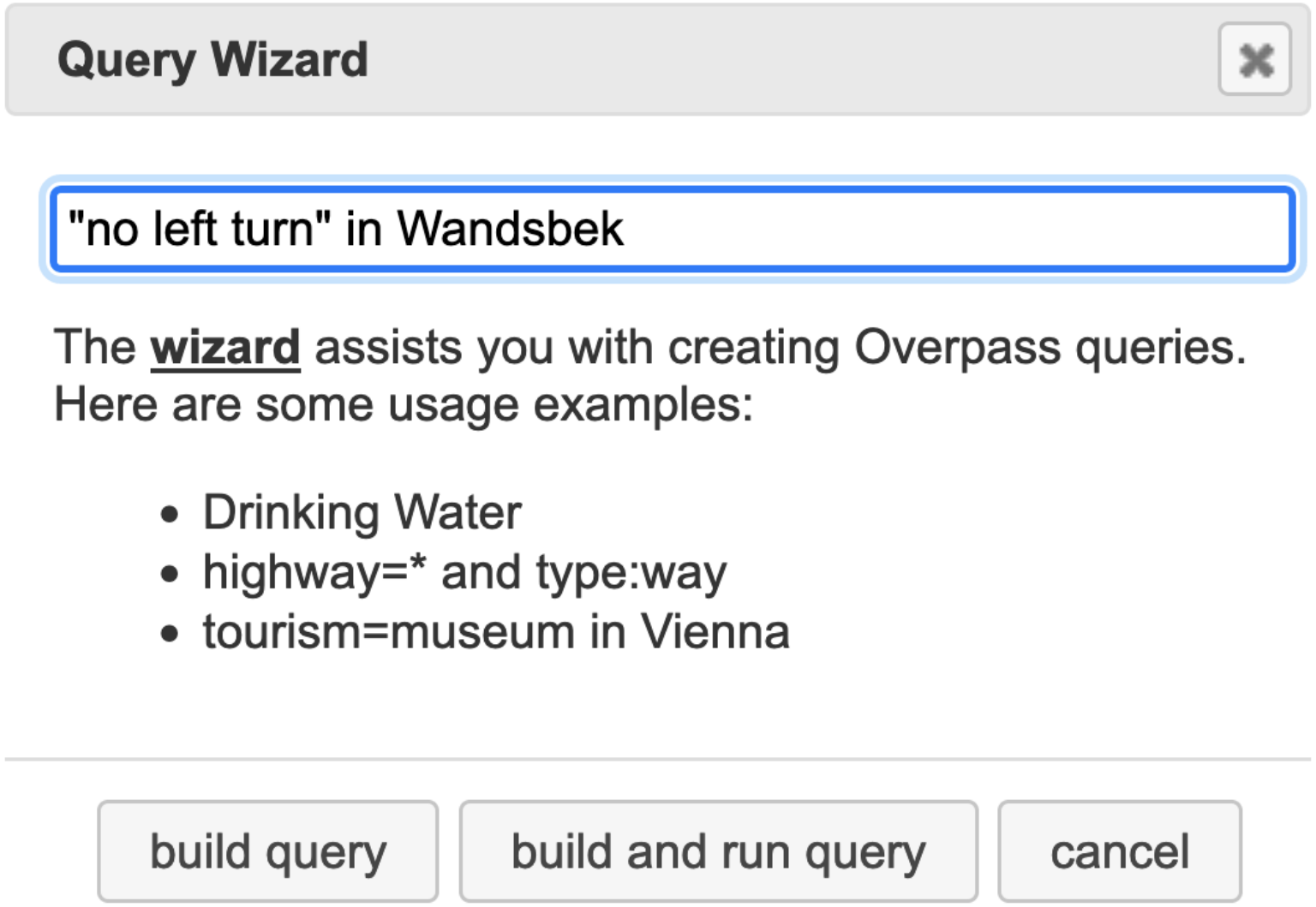
OpenStreetMap

- Die ganze Welt in einer Geodatenbank
- In Metropolregionen auch detaillierte Abdeckung
- Lässt sich nach Objekten anhand ihrer Eigenschaften durchsuchen! z.B.
  - Beschaffenheit von Straßen und Wegen
  - Anzahl Fahrstreifen
  - Ampeln
  - Verkehrsregeln
  - Briefkästen, Bushaltestellen, Werbetafeln, Automaten, …

@dondude, Twitter: "Where did I find this piece of poetry?"


Laterne
Gebäude
Vorgeschriebene Fahrtrichtung
Vorfahrtstraße
Fuck and Listen to Joy Division
Ampel
Bäume
Laterne
Straße
Grünfläche
Geländer
3 Fahrstreifen
Verkehrsinsel
2 Fahrstreifen
Pflasterstein-Seitenstreifen
Grünfläche
Gehweg

restriction	Deutsche Entsprechung	Verkehrzzeichen
only_right_turn	Nur rechts	
only_left_turn	nur links	
only_straight_on	nur gerade	
no_left_turn	nur gerade und rechts! (Anm. 3)	
no_right_turn	nur gerade und links! (Anm. 3)	
no_straight_on	nur links und rechts! (Anm. 3)	
no_u_turn	Wendeverbot	
no_entry	Einfahrverbot	


Query Wizard
"no left turn" in Wandsbek
The wizard assists you with creating Overpass queries.
Here are some usage examples:
Drinking Water
highway=* and type:way
tourism=museum in Vienna
build query
build and run query
cancel

Run | Share | Export | Wizard | Save | Load | Settings | Help

overpass turbo

Map | Data

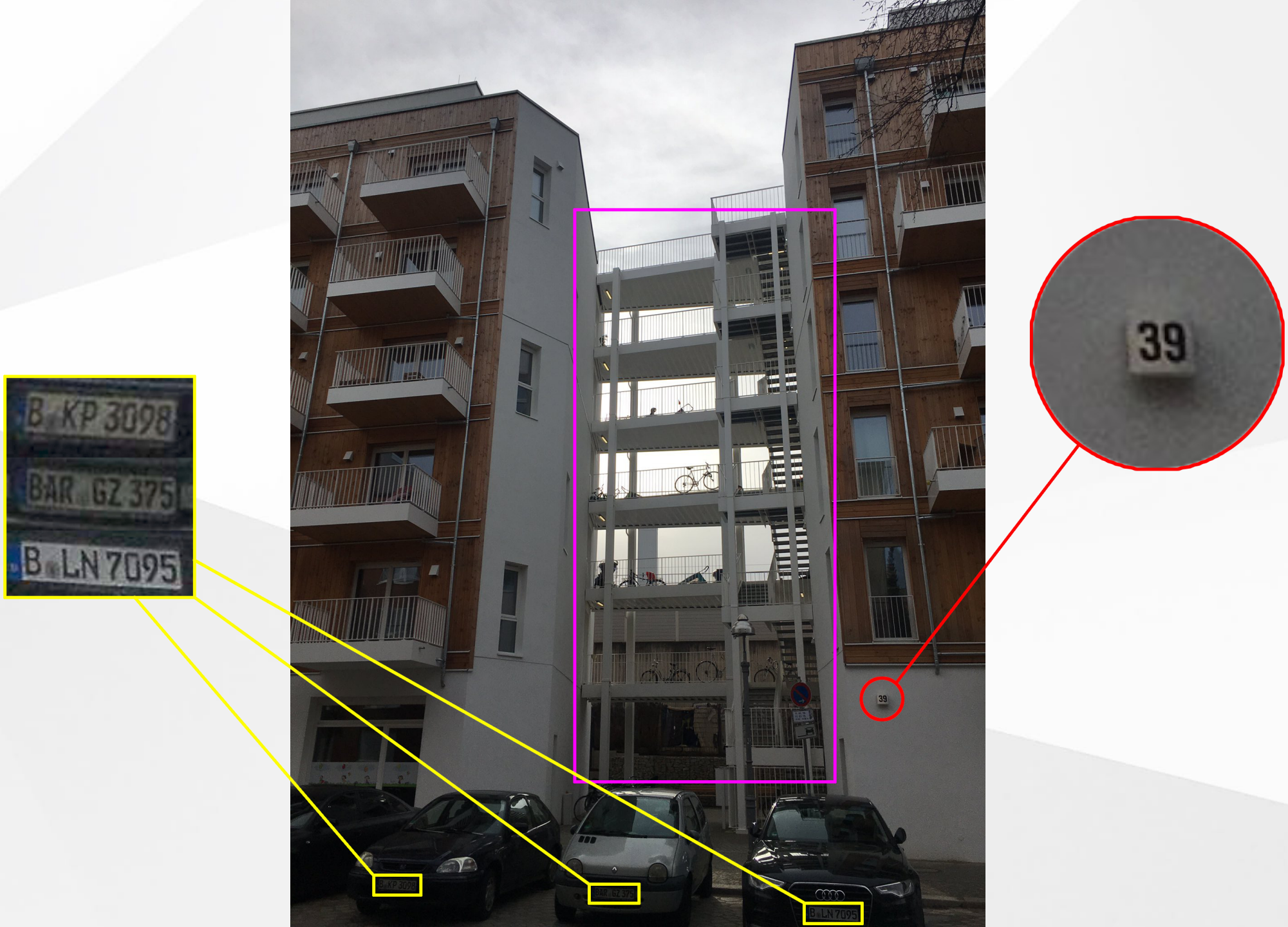
```
{{geocodeArea:Wandsbek}}->.searchArea;


relation
  [type=restriction]
  [restriction=no_left_turn]
  (area.searchArea);

out body;
>;
out skel qt;
```

Loaded – nodes: 104, ways: 30, relations: 16

Displayed – pois: 14, lines: 30, polygons: 0

Mapillary
Sign in or Sign up
AUTOMAT
Parkschein
hier lösen
PT 98
3D
Image by mjay
Aug 17, 2017

@bayer_julia, Twitter: "Where did I take this picture?"


B KP 3098
BAR GZ 375
B LN 7095
39

Run | Share | Export | Wizard | Save | Load | Settings | Help

overpass turbo

Map | Data

```
way[building=bridge];

node(around:10)
  ["addr:housenumber"=39];


out;
```

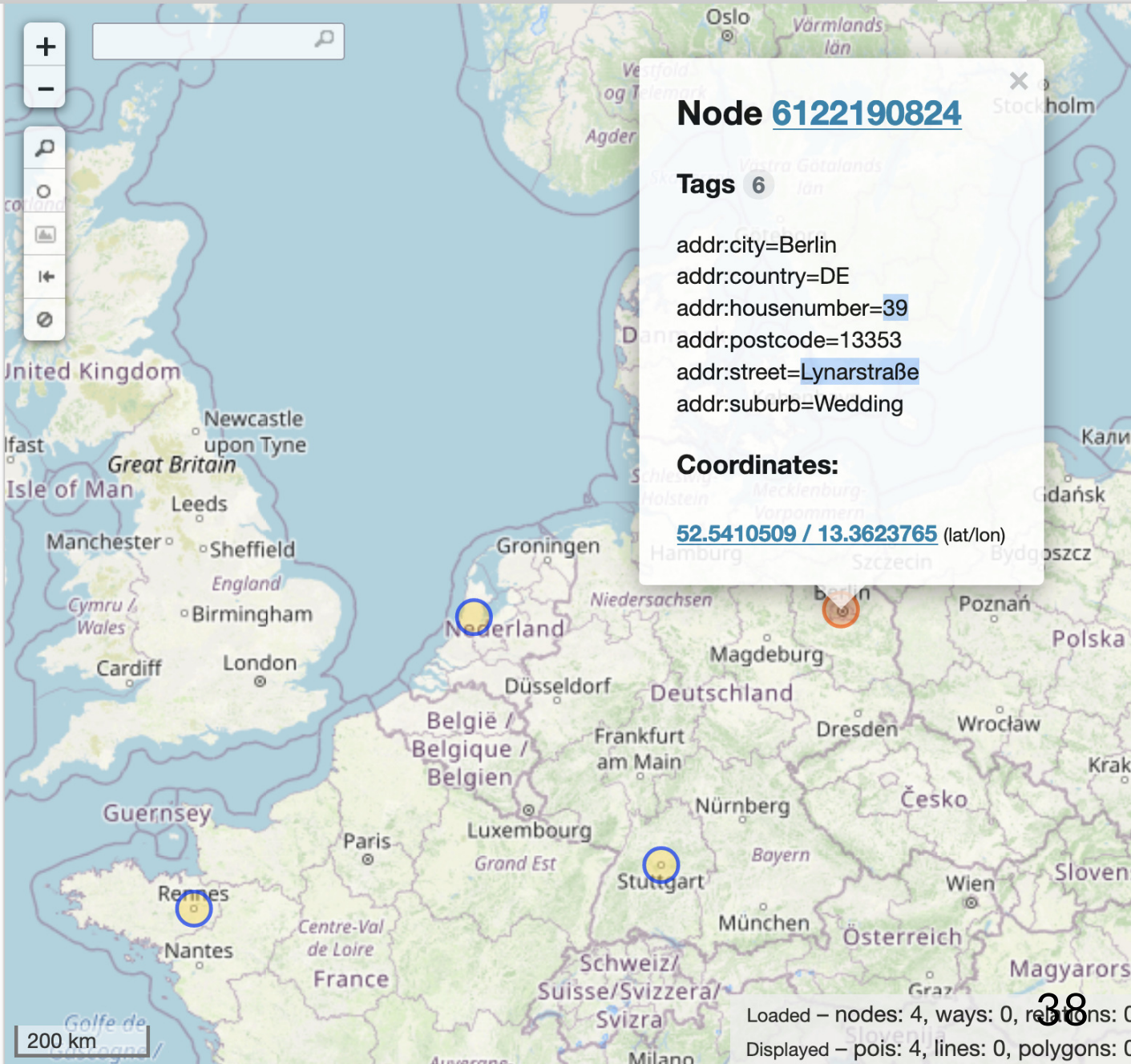


Bild-Datenbanken

- Google StreetView, Mapillary, OpenStreetCam
- Google Places, Foursquare, Yelp, Tripadvisor
- Reiseportale
- Immobilienportale, WG-Suche, Gastfreundschaftsnetzwerke
- Flickr, 500px, Photobucket
- Wikimedia Commons
- Instagram, Twitter, Facebook, Snapchat
- Webcam-Seiten
- YouTube

Kartendaten und Luftbilder

- OpenStreetMap
  - iD und JOSM haben viele Karten- und Luftbilder hinterlegt
- Google Maps (Street)
- Google Maps (3D) / Google Earth
- Kommunen und Länder ("Geoportal")
  - Oft detaillierte Eigenschaften von Gebäuden u. A.
  - Hochauflösende Orthofotos oder Schrägluftbilder
- Sentinel Hub, zoom.earth, Google Earth "Explore New Satellite Imagery"

Social Media & Co

- Follower-Analyse
- Metadaten-Analyse
- Username-Recherche
- Emails & Passwörter
- Inhalte Analysieren

Follower-Analyse

- Erste Follower sind oft IRL Bekannte
- Bekannte recherchieren
  - Wohnort
  - Schule
  - Arbeitgeber
  - Sport, Vereine, Hobbies
  - Fotos

Metadaten-Analyse

- Wann wird üblicherweise gepostet (Anwesenheit / Abwesenheit)
- Wie wird gepostet (Android App, iOS App, Browser, ...)
- Wann wird regelmäßig gepostet
- Wann wird regelmäßig **nicht** gepostet
- Gibt es Abweichungen / Unregelmäßigkeiten?

→ "SpiegelMining" von David Kriesel @ 33C3

Username-Recherche

- Welche Usernames werden verwendet?
- Welche Usernames wurden früher verwendet?
  - Antworten mit @mentions unter alten Posts
  - Datenbanken, insbesondere Online Games
  - Google Cache, Web-Archives, Scraping-Webseiten
- Wo sind diese Usernames registriert?

Emails & Passwörter

- You have been pwned! Fast jeder war mal von Datenleck betroffen
- Welche Email-Adressen wurden verwendet?
  - Welche Accounts verwenden dieselbe Email-Adresse?
- Welche Passwörter wurden verwendet?
  - Welche Accounts verwenden dasselbe Passwort?
- "Passwort vergessen"
  - Zeigt Email-Adressen und Telefonnummern (ganz oder teilweise)
- Gravatar
  - Profilbild ist `md5(email)`. → Nach `md5(email)` im Netz suchen!

How do you want to reset your password?

President Trump
@POTUS

We found the following information associated with your account.

- Email a link to **ds******************@gmail.com**

Continue

Inhalte Analysieren

- Mit wem wird häufig interagiert?
- Welche Themen / Hashtags werden benutzt?
- Welche Sprachen werden benutzt?
- Wiedererkennbare Rechtschreib- und Grammatikfehler?
- Wörter, die nur in bestimmten Regionen verwendet werden?
- Suche nach speziellen Begriffen
  - "ich wohne in", ...
  - "arbeit", "chef", "chefin", ...
  - "frau", "ehefrau", "freundin", "gf", "ex", ...

Ergebnisse verifizieren

- Ergebnisse basieren oft auf wildem Herumsuchen und Raten
- Sind unsere Ergebnisse wirklich richtig?
- Vielleicht nur ein ähnlicher Treffer?
  z.B.
  - Anderer Benutzer mit identischem Namen
  - Anderes Haus mit identischem Baustil
- Können wir beweisen, dass die Daten übereinstimmen?

I have keys

- GitHub und GitLab erlauben `.keys` hinter dem Username
  - Gibt alle SSH-Keys des Nutzers aus
  - Auch bei privaten Instanzen 🤦
    (HEISST JA AUCH PUBLIC KEY !1!!)
  - Public Key reicht aus, um SSH-Server nach Akzeptanz zu fragen
    (`USERAUTH_REQUEST`)
- PGP-Keyserver sind gute Email-Datenbanken
  - Oft werden identische Schlüssel für private und berufliche oder andere Adressen verwendet

Git-Repos sind gute Datenbanken

- Commits enthalten Name, Email-Adresse und Zeitzone
  - Oft Mail-Adressen der Hochschule oder Arbeitgeber
  - In Verbindung mit Realname
  - Oder alte Nicknames und Deadnames
- Profildaten bei GitHub & Co ändern hilft nicht
- Force-push reicht nicht aus
  - In Forks und Pull-Requests bleiben die Daten erhalten

Hostnames

- TLS-Zertifikate
  - Enthalten alle Domains / Subdomains, für die das Zertifikat gültig ist
  - Werden öffentlich protokolliert
    - Suchmaschine: https://crt.sh
- DNSSEC
  - `NSEC`-Records enthalten den Namen des nächsten Eintrags
  - Einträge lassen sich enumerieren

WiFi

- Ja, Wardriving gibt es noch
  - WiGLE.net, Radiocells.org
  - Standortbestimmung von WLAN-Netzen anhand des Namens

Ich weiß wo dein Haus wohnt

- Vortrag kratzt nur an der Oberfläche!
- Postet nicht alles ins Internet!
- Feind hört mit; Silence means Security!
- Lasst alle Infos aus, die nicht relevant sind!
- Alles was Sie sagen, kann und wird gegen Sie verwendet werden!

Tools & Infos

- https://github.com/jivoi/awesome-osint — Große Sammlung
- https://cipher387.github.io/osint_stuff_tool_collection/ — Große Sammlung
- https://bellingcat.com — OSINT-Journalismus mit detailreichen Erklärungen und eigenen Tools und Anleitungen
- https://osintframework.com — Toolsammlung
- https://osintcurio.us — Tipps und Anleitungen
- https://sector035.nl — "Week in OSINT"
- https://nixintel.info/ — Tipps und Anleitungen

Interesse geweckt?

- @quiztime auf Twitter folgen
  - Jeden Tag eine OSINT-Challenge
  - Macht spaß
  - Man lernt viel

Danke für's Zuhören!

Habt ihr Fragen?

Mastodon	@jomo@mstdn.io
Twitter	0xjomo
IRC	jomo @ {hackint, libera, oftc, ~~freenode~~}
Email	osint@jomo.tv