Online-Recherche

Boris Kartheuser

Journalismus und Recherche

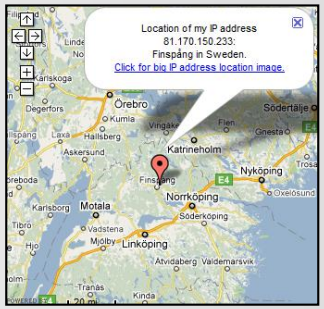
BY NC ND

IP-Adressen

Bei Wunsch nach Anonymität unbedingt beachten:

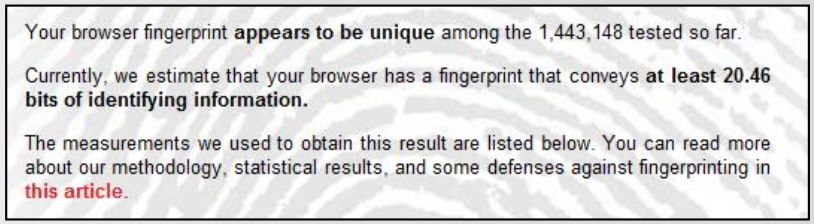
Die eigene IP-Adresse …

ip-adress.com



… in Kombination mit Browserinformationen…

panopticlick.eff.org



Your browser fingerprint **appears to be unique** among the 1,443,148 tested so far.

Currently, we estimate that your browser has a fingerprint that conveys **at least 20.46 bits of identifying information.**

The measurements we used to obtain this result are listed below. You can read more about our methodology, statistical results, and some defenses against fingerprinting in **this article**.

… Tracking - Cookies etc…

…kann eine Identifizierung des Seitenbesuchers ermöglichen. Auch Mails enthalten im Header IP-Informationen. Entweder ein Virtual Private Network (VPN) mit einem User Agent Switcher nutzen oder bei besonders kritischen Recherchen TAILS.

Suchmaschinen-Operatoren

- **Minuszeichen:**
  Mit einem Minuszeichen (ohne Abstand) schließt man (beliebig viele) Begriffe von der Suche aus:
  Köln -Dom -Rhein

- **Anführungszeichen:**
  Man kann Wörter in Anführungszeichen setzen. Sie stellen sicher, dass der Inhalt genau so geschrieben wird und erlauben das Suchen nach Wortgruppen
  „George Bush“ -„George W. Bush“ -„George H.W. Bush“

- **Wildcard**
  Man kann * als Platzhalter innerhalb der Anführungszeichen verwenden:
  *„der Dom ist * Meter hoch“*

- **URL einschränken**
  Der „site:“-Befehl grenzt die Suche auf bestimmte Webseiten ein:

nur Top Level Domain (tld):	*site:de*
ganze Domain:	*site:sueddeutsche.de*
erweiterte Domain:	*site:spiegel.de -site:spiegel.de/wirtschaft/unternehmen*

  Wichtig: kein http://www. XYZ.com/index.html

Suchmaschinen-Operatoren

- **Dokumententyp:**

  Der Befehl „filetype:“ grenzt den Dokumententyp ein:

  filetype:doc (oder pdf, xls, ppt, txt, rtf…)

- **Der Operator OR:**

  Mit dem Befehl „OR“ mit Abstand wird festgelegt, dass nach mindestens einem von mehreren Begriffe gesucht wird:

  filetype:doc OR filetype:pdf

  site:de OR site:fr

Operatoren können **kombiniert**…

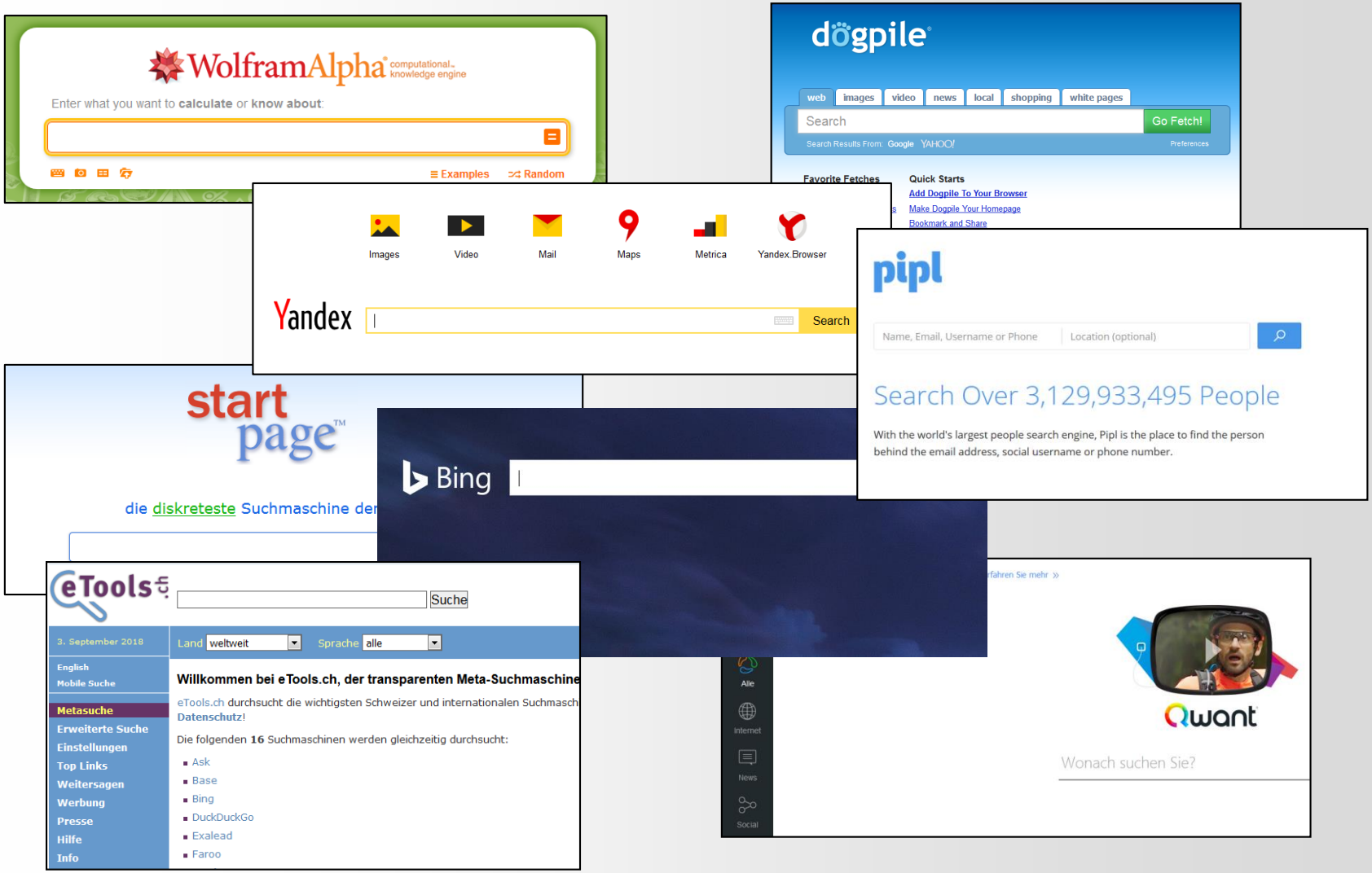
Merkel -Angela site:de OR site:fr OR site:it -site:spiegel.de filetype:doc OR filetype:pdf

…und eine Suche mit **Datum** eingegrenzt werden:

after:2012/2/28 before:2012/12/31

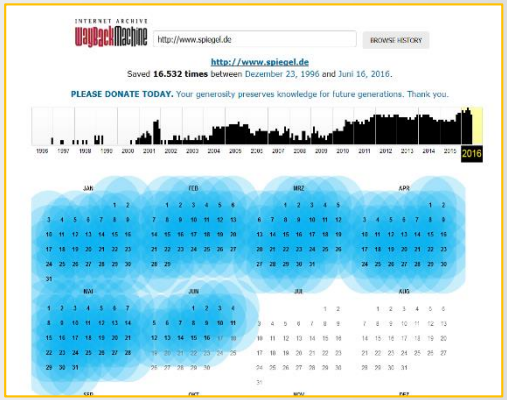
siehe auch allinanchor:, allintext:, allintitle:, allinurl:, cache:, define:, id:, inanchor:, info:, intext:, inurl:, link:, related: etc…

Suchmaschinen - Vielfalt

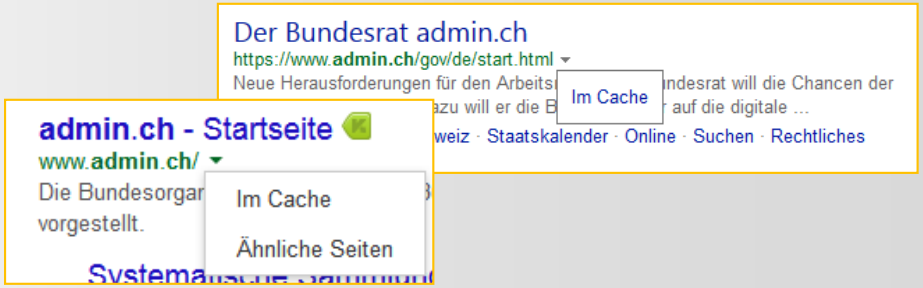


Suchmaschinen - Archive

- Die meisten archivierten Seiten finden wir mit der Waybackmachine. Die bietet auch eine Suchfunktion für das gesamte Archiv.



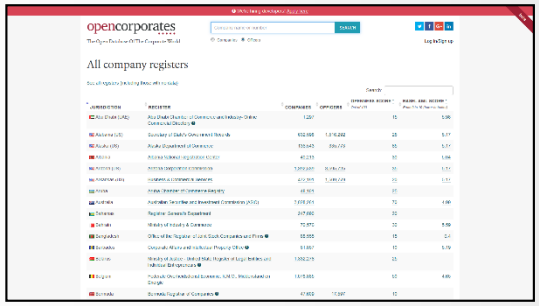
- Bing, Google und Co haben jeweils ein eigenes simples Archiv, Cache genannt, das andere Informationen enthalten kann, als das der Konkurrenten!



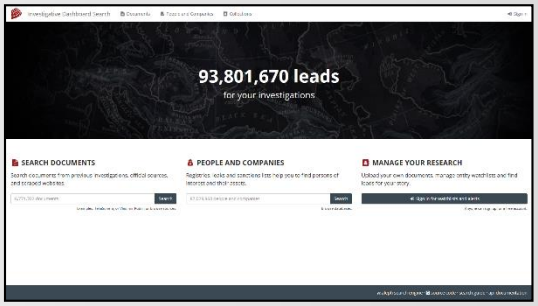
- Alternative Archive : List of Web archiving initiatives

Datenbanken

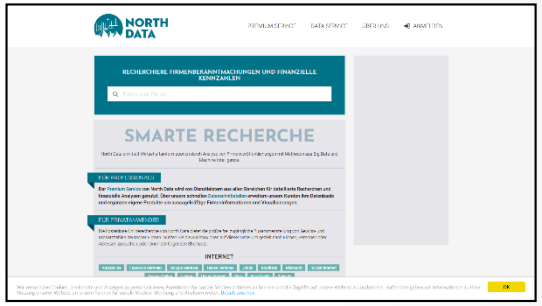
opencorporates.com



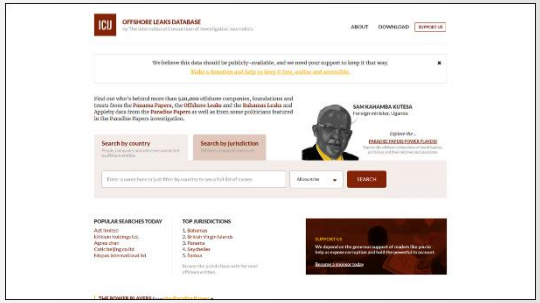
data.occrp.org



northdata.de



https://offshoreleaks.icij.org



openownership.org

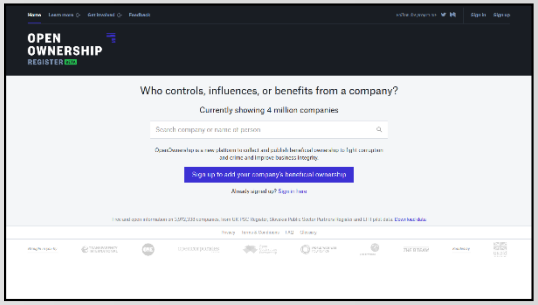


Bild-Verifikation

- Eigene Augen benutzen und Dinge kritisch hinterfragen. Den Ort genau ansehen mit Google Earth Pro, Bing Bildersuche, Terraserver-Satellitenbildern und Co. Praktisch ist das Chrome-Addon Map-Switcher. Das Wetter überprüfen mit Wolfram Alpha

- Rückwärts-Bildersuche mit Addon. Die Suchmaschine Yandex ist dazu derzeit besonders geeignet. Bei der Suche nach Gesichtern vorher remove.bg verwenden und den Hintergrund entfernen. Ist nur der Hintergrund wichtig, dann das Gesicht vorher verpixeln. Dadurch erzielt man bessere Treffer.

- Metadaten untersuchen mit Exif-Viewer

- Unterschiede bei Fotos untersuchen mit DiffChecker

- Logos suchen mit dem Logo Detector

- Text aus Fotos online mit Soda OCR

- Gebäude finden mit Phorio.com

- Videos zu großen Fotos umfunktionieren mit Image Composite Editor

- Fortgeschrittene können sich herantasten an Error Level Analysis und Clone Detection bei Fotoforensics

Üben kann man bei First Draft!

Facebook Search

In den Einstellungen unbedingt die Sprache auf **English (US)** stellen!

- Die eigene Suche bei Facebook bietet mittlerweile einige Möglichkeiten

- Man erhält mehr Foto- Resultate, wenn man die Quelle einstellt

- OCR der Fotos funktioniert ab Februar 2019, besser aber ab Oktober 2019 (Nummernschilder, Telefonnummern etc.)

- In der Suchbox keyword suchen, dann Source auswählen. Bei einer weiteren Suchen mit der gleichen Quelle in der URL über q= ändern. Abstand oder %20 bei mehreren Begriffen

- die neuesten Posts zu einem Thema finden
  https://www.facebook.com/search/latest/?q=SUCHBEGRIFF%20SUCHBEGRIFF%20SUCHBEGRIFF

- Wenn es komplexer wird: https://whopostedwhat.com und https://sowdust.github.io/fb-search (dazu bei Facebook einloggen)

- Du willst viel viel mehr? Hier steht, wie es geht:
  https://osintcurio.us/2019/08/22/the-new-facebook-graph-search-part-1

  Zum Beispiel *'John', who lives in 'Mountain View', who works for 'Google'!*

  facebook.com/**search/people**/?q=**john**&epa=FILTERS&filters=**eyJjaXR5Ijoie1wibmFtZVwiOlwidXNlcnNfbG9jYXRpb25cIixcImFyZ3NcIjpcIjEwODIxMjYyNTg3MDI2NVwifSIsImVtcGxveWVyIjoie1wibmFtZVwiOlwidXNlcnNfZW1wbG95ZXJcIixcImFyZ3NcIjpcIjEwNDk1ODE2MjgzN1wifSJ9**

Twitter Suche

Viele Suchmaschinen-Operatoren wie OR , Minus oder Anführungszeichen funktionieren auch in der Twittersuche

darüber hinaus…

- ***from:****Benutzername* *(alternativ bei Google site:twitter.com/Benutzername)*
- ***lang****:de* sucht (unzuverlässig) nach Tweets, die als Deutsch eingeordnet werden (lang:en entsprechend nur englisch)
- ***since****:2012-01-01* oder ***until****:2012-12-31* *auch eher unzuverlässig…*
- weitere Möglichkeiten: https://twitter.com/search-advanced?lang=de

Viele weitere Operatoren findest du bei labnol.org (*site:labnol.org best twitter tricks*)

Die wohl hilfreichste Einschränkung läuft mit dem *geocode:* Operator bei Twitter: mit Diensten wie mygeoposition.com oder Google Maps (rechte Maustaste auf Ort – „Was ist hier“) den Längen- und Breitengrad bestimmen und nur den ausgesuchten Ort nach Tweets durchsuchen. Nicht vergessen, einen Umkreis anzugeben:

geocode:52.5186200,13.3761870,0.5km

geocode:53.5125960,14.5784788,2km

Twitter - Geolocation

=> sollen Bilder enthalten sein, Suchbegriffe entsprechend ergänzen um Dienste wie *instagram.com*

Beispielsweise Bilder vom Kölner Dom:

Dom OR cathedral geocode:50.9412935,6.9580901,0.5km *url:instagram.com*

Oder den filter:-Operator verwenden

Dom OR cathedral geocode:50.9412935,6.9580901,0.5km filter:images

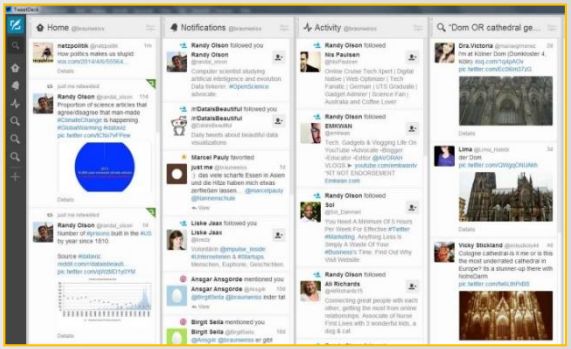
Alternativ Tools wie das Python-basierte Creepy nutzen, zum Beispiel vorinstalliert beim Live-Linux Buscador

Oder Bezahldienste wie Echosec

Twitter Suche

- Dienste wie tweetdeck.com erleichtern die tägliche Arbeit mit Twitter und bieten komfortable Suchmöglichkeiten.

  Besonders hilfreich ist es Listen zu erstellen und diese einfließen zu lassen. Die können dann wieder gefiltert werden.

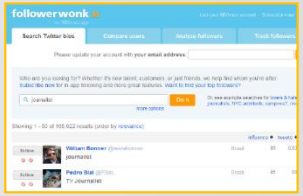


- Listen finden mit Google-Suche: site:twitter.com/*/lists inurl:THEMA

Twitter Suche

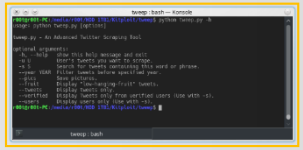
Einen Überblick über die Kontakte des Twitterers, das Anmeldedatum und über seine getwitterten Themen bietet foller.me

Die Eigenangaben der Twitternutzer und Beziehungsgeflechte kann man mit followerwonk.com durchsuchen. Nützlich bei der Suche nach Berufsgruppen oder Nutzern in bestimmten Wohnorten.



Tinfoleak bietet jede Menge Informationen über Nutzer. Manchmal auch geolocation. Besorg dir die hierfür benötigte Mail-Adresse bei 10minutemail.com

Wer unlimitiert Tweets scrapen will, kann das mit dem Python-basierten Tweep tun



Netzwerkanalyse mit Bezahltools wie Scraawl

Listen finden mit Google-Suche: site:twitter.com/*/lists inurl:THEMA

Instagram

Schnelles Durchsuchen mit Google und Co:

- Posts, manchmal auch private: *"instagram.com/p/" „USERNAME“*
- Benutzername und Stichwort: *site:instagram.com „USERNAME" „KEYWORD"*
- Erwähnungen: *site:instagram.com "@USERNAME" -site:instagram.com/USERNAME*
- Mehrere Suchbegriffe/ Hashtags: *site:instagram.com „KEYWORD" „KEYWORD"*

Anonsten:

- Mit www.mulpix.com nach mehreren Keywords suchen
- Mit www.instadp.com Userbilder in groß für reverse image
- Mit www.searchmy.bio UserBios durchsuchen
- Mit https://bigsta.net/location Geolocation durchsuchen
- Mit getip.social versuchen, Registrierungsdatum des Instagram-Kontos herausfinden (hakt manchmal)
- Mit www.statflux.com Nutzerinformationen finden (hakt manchmal)
- Location und Zeit: https://www.osintcombine.com/instagram-explorer
- Mit skimagram.com nach Insta-Videos zu Hastag suchen

Instagram

Chrome Addons:

Desktop for Instagram
Offered by: www.devanco.com

hier

„This app allows you to access to the Instagram mobile website like you can do on your smartphone but on your computer"

(Firefox: Addon mobile-view-switcher)

Downloader for Instagram™
Offered by: aboveradiant

hier

„download photo, video and stories, view Live, mass download, direct message, upload photo."

Helper Tools for Instagram v2
Angeboten von: helpertoolsforinstagram.com

(teils kostenpflichtig)

hier

„Create list of followers/following of an Instagram account, find common users of 2 IG accounts, calculate likes/comments on profile, hidden connection between Instagram users" Bei business accounts Kontakt

Oder mit Tools wie InstagramOSINT (Python) alle Fotos und Videos runterladen

LinkedIn

- In der Linkedin-Suche selbst kann man Operatoren verwenden wie AND, OR (Anführungszeichen), „Klammer“, company: , profilelanguage: , yoe: (years of experience) - derzeit nur 4 Operatoren pro Suche bei basic account möglich!

- Nutze https://recruitin.net um Linkedin mit Hilfe von Google zu durchsuchen (Country, Job title, key words etc)

- Mit Chrome Extensions wie ContactOut oder Lusha Kontaktdaten auslesen

- Mit linkedin.com/sales/gmail/profile/viewByEmail/Beispielmailadresse den Kontakt zu einer Mail finden. Emails herausfinden mit hunter.io

- Den Seitenquelltext öffnen und nach “postalCode&quot” suchen! Manchmal findet man damit die Postleitzahl

- Mit Python und LinkedInt, ScrapedIn oder inspy Linkedin scrapen

Xing

- site:xing.com/profile/ intitle:„BERUF" „STADT"

- Nicht freigegebene Kontakte einer Zielperson kann man sichtbar machen, indem man die Person als einzigen Kontakt gewinnt oder übrig lässt und im Falle einer gesuchten Kontaktperson beispielsweise den Pressesprecher des Unternehmens einsetzt. Xing sucht jetzt alle möglichen Verbindungen.

- Man kann auch den umgekehrten Weg gehen und eine Liste möglicher Verdächtiger als Kontakt gewinnen und in Xing dann nach der Zielperson suchen.

IP-Recherchen

Whois

Wer hat die Seite angemeldet?

für .de: denic.de (als Journalist anfragen)
für .info, .net, .com…: whois-search.com versuchen
Vergangenheit: whois.easycounter.com versuchen
oder:
https://web.archive.org/web/*/https://who.is/whois/BEISPIEL.XYZ

Domaincheck

Welche anderen TLDs sind belegt?

checkdomain.de

Reverse IP

Was liegt dort noch?

derzeit defekt:
~~IP der Seite ermitteln z.B. mit Addon Flagfox und dann in der Bing-Suche eingeben: IP:62.138.XXX.X~~

IP-Tracking

Serverstandort

Flagfox oder ip-adress.com

alternativ Dienste wie tcpiutils oder Bezahldienste wie cybertoolbelt oder domaintools

Viele weitere nützliche Ressourcen…

…finden sich auf http://www.investigativerecherche.de/ressourcen