
PRAXISLEITFADEN · ÖSTERREICHBEZUG · OFFENE COMMUNITY

OSINT-Kompass

Quellen prüfen.
Spuren verstehen.

Offene Quellen sind ein Anfang. Dieser Leitfaden zeigt, wie Sie daraus begrenzte, nachvollziehbare Aussagen entwickeln: mit Methoden, kommentierter deutschsprachiger Fachlektüre und einem echten Webseitenvergleich zum Nacharbeiten. Die Community hält Wissen zugänglich und entwickelt Werkzeuge gemeinsam weiter.

Thomas Lechleitner, MSc

17 Kapitel · Praxisbeispiele · kommentierte Fachlektüre
Redaktioneller Stand: 12. Oktober 2026

Ehrenamtliches Informationsangebot von noctuaforensis.
Keine persönliche Fallbearbeitung; kein unabhängiges Fachgutachten.

Inhalt und Hinweise

00 · Warum dieser Leitfaden	3
01 · OSINT und digitale Forensik unterscheiden	4
02 · Wie sich Recherche verändert hat	5
03 · Ein Arbeitsablauf mit Rückkopplung	6
04 · Recht und Ethik in Österreich	7
05 · Das OSINT Framework sinnvoll verwenden	8
06 · Benutzernamen, Konten und Identität	9
07 · Domains und technische Infrastruktur	10
08 · Bilder, Metadaten, Ort und Zeit	11
09 · Werkzeuge nach Aufgabe auswählen	12
10 · Die Community als dauerhafte Grundlage	13
11 · Selbstschutz und Schutz anderer	15
12 · Von der Beobachtung zur begrenzten Aussage	16
13 · Wenn die Recherche nicht weiterführt	17
14 · Drei durchgearbeitete Praxisbeispiele	18
15 · KI und Automation mit überprüfbarem Nutzen	20
16 · Glossar und nachprüfbare Quellen	21

Diese PDF ist eine lesefreundliche Fassung des vollständigen OSINT-Kompasses. Die Kapitelnummerierung entspricht der Webseite. Das separate, echte Übungspaket bleibt online abrufbar.

Externe Links: Beim Öffnen von Quellenlinks verlassen Sie das Angebot von noctuaforensis. Inhalte und Datenverarbeitung dieser Dienste liegen in der Verantwortung der jeweiligen Anbieter. Der Hinweisdialog der Webseite ist innerhalb einer PDF technisch nicht verfügbar.

Aktuelle Webfassung · Echter Webseitenvergleich mit Übungspaket

00 · Warum dieser Leitfaden

Eine Suche liefert schnell einen Namen, ein Bild oder eine IP-Adresse. Schwieriger ist die Frage, was ein solcher Fund tatsächlich belegt. Dieser Leitfaden soll dabei helfen, den nächsten sinnvollen Schritt zu wählen und rechtzeitig zu erkennen, wann die eigene Schlussfolgerung weiter reicht als das Material.

Thomas Lechleitner, MSc bündelt hier Grundlagen, Werkzeugkunde und praktische Arbeitsweisen. Der Schwerpunkt liegt auf verantwortungsvoller Recherche, digitaler Forensik und dem österreichischen Kontext. Das OSINT Framework dient als Orientierung; der Lernweg führt von der Fragestellung über Quellen und Gegenprüfung zum Bericht.

Was über einzelne Werkzeuge hinaus bleibt

Die Beständigkeit von OSINT liegt wesentlich in seiner Community: Menschen pflegen offene Werkzeuge, berichtigen Erkennungsregeln, übersetzen Anleitungen und geben Erfahrung weiter. Einzelne Dienste können verschwinden. Öffentlich dokumentiertes Wissen kann weiterentwickelt und von anderen aufgegriffen werden. Diese Kontinuität entsteht durch Arbeit und Beteiligung - sie ist keine Garantie, dass jedes Projekt dauerhaft betreut wird.

Wie diese Gemeinschaft Wissen erhält >

Der Leitfaden ist ein ehrenamtliches Informationsangebot. Es ersetzt weder eine professionelle Untersuchung noch die Beratung in einem persönlichen Fall. Für den Einstieg genügt eine kleine, rechtmäßig gewählte Übung. Eine große Werkzeugliste ist dafür nicht erforderlich.

01 · OSINT und digitale Forensik unterscheiden

Open Source Intelligence bezeichnet hier die methodische Auswertung rechtmäßig zugänglicher offener Informationen für eine bestimmte Fragestellung. Recherche wird erst dann aussagekräftig, wenn Herkunft, Zeitpunkt, Zusammenhänge und Unsicherheit der Fundstellen berücksichtigt werden.

„Open Source“ bezieht sich in diesem Begriff auf den Zugang zur Quelle. Es bedeutet nicht, dass sämtliche verwendete Software quelloffen ist oder dass alle Informationen kostenlos und frei weiterverwendbar wären. Auch entgeltliche Registerauskünfte oder allgemein zugängliche Fachpublikationen können offene Recherchequellen sein; Zugang und Nutzungsrechte sind gesondert zu prüfen.

Zwei Arbeitsfelder mit Überschneidungen

OSINT kann etwa öffentliche Veröffentlichungen, Registereinträge oder Zertifikatsbeobachtungen auswerten. Digitale Forensik untersucht rechtmäßig verfügbares digitales Material und legt besonderen Wert auf Erhaltung, nachvollziehbare Verarbeitung und die Grenzen des Befunds. Die lokale Analyse einer eigenen Bilddatei ist eine Übung in Metadatenanalyse; sie wird nicht allein durch den Einsatz eines „OSINT-Tools“ zu Open Source Intelligence.

SOCMINT bezeichnet den Schwerpunkt auf sozialen Medien. GEOINT umfasst geografische und bildbasierte Informationen. Die Bereiche können sich überschneiden. Für die praktische Arbeit ist meist entscheidender, welche Quelle genutzt wird und welche Aussage sie erlaubt, als welcher Sammelbegriff darübersteht.

Unsere redaktionelle Position

Eine große Datenmenge macht eine Recherche nicht automatisch gut. Ein eng begrenzter, nachvollziehbarer Befund ist oft hilfreicher als eine beeindruckende Sammlung ungeklärter Verbindungen.

02 · Wie sich Recherche verändert hat

Bibliotheken, Presse, Register und öffentlich ausgestrahlte Rundfunkprogramme dienten schon vor dem Web als Informationsquellen. Digitale Suchmaschinen und Archive erleichterten später das Auffinden und Vergleichen von Veröffentlichungen. Soziale Netzwerke und technische Verzeichnisse erweiterten den Bestand erneut.

Die Menge der verfügbaren Informationen ist gewachsen; die grundlegenden Fragen bleiben: Wer hat etwas veröffentlicht? Wann? Mit welchem Zugang zum Geschehen? Und welche andere Quelle kann die Aussage stützen oder widerlegen?

Heute verändern neue Plattformregeln, kostenpflichtige APIs und automatische Inhalte die Arbeitsbedingungen. Daraus folgt kein linearer Fortschritt. Manche Quellen werden leichter zugänglich, andere verschwinden. Offene Dokumentation und gepflegte Community-Projekte helfen, Erfahrungen über solche Wechsel hinweg zu erhalten. **Kapitel 10 beschreibt diese Arbeit genauer.**

03 · Ein Arbeitsablauf mit Rückkopplung

Der folgende Kreislauf ist eine praktische Arbeitsstruktur. Er lässt sich an kleine Übungen und größere Aufträge anpassen. Bei neuen Widersprüchen geht es zurück zur Fragestellung oder zur Sammlung.

1. **Planen:** Frage, Berechtigung, Zeitraum und benötigte Daten festlegen. Dazu gehört eine Stoppregel: Wann reichen die Informationen, und welche Recherche wäre unverhältnismäßig?
2. **Sammeln:** Geeignete Quellen wählen und Herkunft sowie Abrufzeit mit Zeitzone festhalten. Veröffentlichungszeit, Zeitpunkt des Ereignisses und eigene Abrufzeit auseinanderhalten.
3. **Aufbereiten:** Dubletten kennzeichnen, Formate vereinheitlichen und Originale von Arbeitskopien trennen. Bei jeder übernommenen Aussage muss die Ursprungsquelle erhalten bleiben.
4. **Analysieren:** Beobachtungen mit der Frage verbinden, alternative Erklärungen prüfen und Grenzen benennen. [Kapitel 12 vertieft die Bewertung.](#)
5. **Berichten und nachprüfen:** Ergebnis für den vorgesehenen Empfänger formulieren, offene Punkte nennen und entscheiden, ob weitere Schritte nötig und zulässig sind.

Eine brauchbare Stoppregel

Für die Frage „Welche Textstellen unterscheiden sich zwischen zwei vorhandenen Fassungen?“ kann ein dokumentierter Vergleich ausreichen. Die Suche nach privaten Beziehungen des Verfassers erweitert den Zweck und beantwortet diese Frage nicht. Ein sinnvoller Arbeitsablauf schützt auch vor der eigenen Neugier.

Zum Protokoll gehören Quelle, Fundstelle, Zeitangaben, Methode, verwendete Version und Ergebnis. [Leere Text- und Tabellenvorlagen stehen im Lernweg bereit.](#)

[Transparent prüfen: APA-Regeln >](#)

04 · Recht und Ethik in Österreich

Öffentliche Auffindbarkeit schafft keine allgemeine Erlaubnis zur Sammlung, Verknüpfung oder Veröffentlichung. Vor einer Recherche sind Zweck, zulässiger Zugang und Rechte betroffener Menschen zu klären. Bei tatsächlichen Fällen können unterschiedliche rechtliche Anforderungen zusammenkommen.

Datenschutz

Bei personenbezogenen Daten sind insbesondere Datenminimierung, Zweckbindung und eine geeignete Rechtsgrundlage zu prüfen. Ein berechtigtes Interesse nach Art. 6 Abs. 1 lit. f DSGVO verlangt eine konkrete Abwägung. Besondere Datenkategorien und Angaben zu strafrechtlichen Sachverhalten unterliegen zusätzlichen Anforderungen nach Art. 9 beziehungsweise Art. 10. In Österreich ist auch das Datenschutzgesetz zu berücksichtigen.

Zugang und Weiterverwendung

Technische Erreichbarkeit ist keine Zugriffsberechtigung. Zugangssperren nicht umgehen und fremde Zugangsdaten nicht ausprobieren. § 118a StGB betrifft widerrechtlichen Systemzugriff unter seinen gesetzlichen Voraussetzungen. Daneben können Urheber- und Datenbankrechte, Persönlichkeitsrechte sowie Plattformbedingungen relevant sein. Ein Screenshot oder ein Archivfund hebt diese Rechte nicht auf.

Verantwortung beginnt vor der Veröffentlichung

Eine Recherche kann Menschen schaden, auch wenn einzelne Informationen öffentlich waren. Private Adressen, Gesundheitsangaben oder unbelegte Verdachtsäußerungen gehören nicht unbedacht in einen Bericht. Überlegen Sie, welcher Empfänger welche Information wirklich benötigt und ob eine anonymisierte Darstellung genügt.

[Rechtliche Grenzen mit österreichischen Primärquellen >](#) · [DSGVO im Quellenverzeichnis >](#) · [§ 118a StGB im RIS >](#)

Allgemeine Orientierung, keine individuelle Rechtsberatung. Bei einem akuten Verdacht keine unüberlegten Veränderungen an möglichen Beweismitteln vornehmen. [Anlaufstellen in Österreich >](#)

05 · Das OSINT Framework sinnvoll verwenden

Das von Justin Nordine begründete OSINT Framework ordnet Recherche-Ressourcen in einer Baumstruktur. Wer beispielsweise eine Domain untersuchen darf, findet Ansatzpunkte zu Zertifikaten, DNS-Beobachtungen oder Archivfassungen. Das Verzeichnis hilft bei der Auswahl; eine Eintragung bestätigt nicht die Qualität eines Dienstes.

Vom Ausgangsobjekt zur nächsten prüfbaren Frage

Ein sogenannter Pivot führt von einer Information zu einer möglichen weiteren Verbindung. Aus einem Zertifikatsnamen kann eine Frage nach einer Subdomain entstehen. Ob diese Subdomain aktuell betrieben wird oder derselben Organisation gehört, ist jeweils ein neuer Prüfschritt. Ein Verzeichnis liefert solche Übergänge, keine fertige Beweiskette.

Projektlegende, am 12. Oktober 2026 mit dem README abgeglichen

Kürzel	Bedeutung	Vor der Nutzung
T	Lokal zu installierendes Werkzeug	Herkunft, Version und Umgebung prüfen
D	Google-Suchoperator / Google Dork	Suchausdruck und Ergebnis einordnen
R	Registrierung erforderlich	Bedingungen und Datenübermittlung prüfen
M	Suchbegriff in der URL manuell anpassen	Parameter ändern; keine Aussage über eine API

Eine lokal gespeicherte Verzeichnisfassung macht die verlinkten Dienste nicht offline verfügbar. Eine Anpassung sollte das Prüfdatenblatt ergänzen: Wer hat den Verweis zuletzt geprüft, was wurde tatsächlich getestet und welche Einschränkung wurde festgestellt?

[Projekt und Legende >](#) · [Praxisbeispiel: historischer Zertifikatsname >](#)

06 · Benutzernamen, Konten und Identität

Sherlock und die auf WhatsMyName-Daten aufbauenden Anwendungen können mögliche Profildaten anzeigen. Die Ergebnisse hängen von Erkennungsregeln und Plattformantworten ab. Eine erreichbare Seite oder derselbe Name belegt keine gemeinsame Person hinter mehreren Konten.

WhatsMyName ist im Kern ein gemeinschaftlich gepflegter Datensatz; unterschiedliche Anwendungen verwenden ihn für die eigentlichen Abfragen. Diese Trennung von Daten und Oberfläche ist ein anschauliches Beispiel dafür, wie Wissen mehrere Werkzeuge überdauern kann. [Projektbeschreibung und Mitwirkung >](#)

Treffer vorsichtig zuordnen

Ein kopiertes Profilbild, ein wiedervergebener Name oder ein gemeinsam benutztes Konto sind mögliche Gegenhypothesen. Eine zusätzliche Übereinstimmung kann helfen, ist aber kein universeller Identitätsbeweis. Erforderliche Personenrecherche braucht einen klaren Zweck; für das Lernen sind eigene oder fiktive Profile die bessere Wahl.

Was ein Datenleck-Hinweis aussagt

Have I Been Pwned kann auf erfasste Datenexpositionen hinweisen. Ein Treffer sagt nicht automatisch, ob ein Konto heute kompromittiert ist; ein fehlender Treffer ist keine Entwarnung. Der öffentliche Adresscheck liefert keine Liste zugehöriger Passwörter. Er ersetzt auch keine Prüfung eines verdächtigen Geräts.

Unsere Grenze ist klar: Keine öffentlichen Persönlichkeitsurteile aus automatischen Fundlisten. Insbesondere die Einstufung einer Person als Sicherheitsrisiko oder Schuldige lässt sich aus solchen Treffern nicht verantwortungsvoll ableiten. [Anbieter-FAQ zum Datenleck-Check >](#)

07 · Domains und technische Infrastruktur

Für eine defensive Recherche an eigenen oder ausdrücklich freigegebenen Systemen sind Registrierungsdaten, DNS-Beobachtungen, Zertifikatsprotokolle und historische Seitenstände nützliche Ausgangspunkte. Die jeweiligen Zeitbezüge entscheiden darüber, welche Aussage möglich ist.

Registrierungsdaten: RDAP und WHOIS

RDAP ist das standardisierte Protokoll für den Zugang zu Domain-Registrierungsdaten und hat WHOIS bei generischen Top-Level-Domains als maßgeblichen Dienst abgelöst. Bei Länder-Domains und einzelnen Anbietern können Zugang und Umfang anders aussehen. Verdeckte oder eingeschränkte Daten sind kein verdächtiger Befund. Registrierungs-, Veröffentlichungs- und tatsächliche Nutzungsdaten sind zu unterscheiden. [ICANN: RDAP >](#)

Zertifikate, DNS und Suchmaschinen

Ein Certificate-Transparency-Treffer belegt einen Zertifikatsbezug. Er bestätigt weder einen aktuellen DNS-Eintrag noch einen erreichbaren Dienst. Passive DNS-Daten zeigen beobachtete Zuordnungen zu bestimmten Zeiten. Eine gemeinsame IP kann zu Hosting, einem CDN oder einem anderen gemeinsam genutzten Dienst gehören.

Shodan und Censys machen eigene Beobachtungen zu technischen Diensten durchsuchbar. Angaben können veraltet oder unvollständig sein. Ein altes Banner liefert eine Prüfidée, aber noch keinen aktuellen Schwachstellenbefund. Die Abfrage eines vorhandenen Index unterscheidet sich von einem selbst gestarteten Scan; direkte Prüfungen benötigen einen passenden Auftrag und Umfang.

Analytischer Stolperstein

Ein Domainname, eine IP und ein Zertifikat können zusammenpassen, ohne denselben Betreiber zu belegen. Zeitliche Übereinstimmung und gemeinsame Infrastruktur müssen gesondert geprüft werden.

[Durchgearbeitetes Beispiel >](#) · [crt.sh als Zertifikatsquelle >](#)

08 · Bilder, Metadaten, Ort und Zeit

Ein Bild kann echt sein und trotzdem eine falsche Behauptung stützen: etwa weil es älter ist, einen anderen Ort zeigt oder ein entscheidender Ausschnitt fehlt. Deshalb gehören technische Prüfung, Bildinhalt und Veröffentlichungskontext zusammen.

Metadaten zuerst lokal betrachten

ExifTool kann vorhandene Metadaten aus vielen Dateiformaten lesen. Je nach Datei finden sich etwa Geräteangaben, Zeitstempel oder Standortinformationen. Solche Angaben können fehlen, verändert worden sein oder aus einer Bearbeitung stammen. Der Standort einer Kamera ist außerdem nicht notwendig der Standort des abgebildeten Motivs.

Bei eigenen rechtmäßig vorhandenen Dateien ist eine lokale Analyse oft ein guter erster Schritt. Die Datei muss dafür nicht zu einem öffentlichen Dienst hochgeladen werden. [Das Bildbeispiel zeigt eine begrenzte Übung.](#)

Bildsuche und Kontextvergleich

Eine Rückwärtssuche kann frühere oder ähnliche Veröffentlichungen sichtbar machen. Eine Nicht-Fundstelle beweist keine Originalität, und ein Trefferdatum ist nicht automatisch das Aufnahmedatum. Vor einer externen Bildsuche prüfen, ob das Bild übermittelt werden darf; die Anbietersuche ist auch eine Datenschutzentscheidung.

Für einen Orts- oder Zeitabgleich helfen erkennbare Gebäude, Landschaft, Beschriftungen und passende Vergleichsbilder. Schatten und Wetter sind ergänzende Hinweise, sofern Blickrichtung und Aufnahmebedingungen bekannt sind. Fehlerlevelanalyse und automatische KI-Detektoren entscheiden nicht allein über Echtheit. [Kapitel 12 zeigt, wie Gegenhypothesen dokumentiert werden.](#)

[Deutschsprachige Bild- und Quellenlektüre >](#)

09 · Werkzeuge nach Aufgabe auswählen

Eine brauchbare Werkzeugwahl beginnt bei der Aufgabe und endet bei einem überprüfbar Ergebnis. „Kann viel“ ist kein ausreichendes Auswahlkriterium. Kleine, verständliche Abläufe lassen sich häufig besser kontrollieren als eine unübersichtliche automatische Sammlung.

Funktionsklassen zur Orientierung; keine Rangliste

Aufgabe	Beispiel	Wichtige Grenze
Quellen finden	OSINT Framework, Bellingcat Toolkit	Verzeichnisaufnahme ist keine Sicherheitsprüfung
Informationen sammeln	theHarvester, SpiderFoot	Quellen, Zugänge und aktive Module vorab prüfen
Mögliche Profile finden	Sherlock, WhatsMyName-basierte Anwendungen	Namensgleichheit ist keine Identitätsbestätigung
Beziehungen darstellen	Maltego, Gephi	Eine Kante muss eine belegte Bedeutung haben
Dateien lokal betrachten	ExifTool, SHA-256-Werkzeuge	Metadaten und Hash bestätigen nicht die Wahrheit des Inhalts

Fünf Fragen vor dem Einsatz

- Welche konkrete Frage beantwortet die Ausgabe?
- Was wird lokal verarbeitet und was an Dritte übermittelt?
- Welche Kosten, Anmeldung oder API-Berechtigung sind nötig?
- Lassen sich Version, Quelle und Verarbeitung dokumentieren?
- Ist eine Fehlermeldung verständlich, oder würde sie als Ergebnis fehlgedeutet?

Automation kann Teilaufgaben abnehmen; sie muss nicht als Nachweis eines höheren Reifegrades gelten. Manchmal ist ein sauberer manueller Vergleich die bessere Wahl. [Lokale Werkzeuge > · Kriterien unseres Katalogs >](#)

[Suchstrategien mit Aktualisierungshinweis >](#)

10 · Die Community als dauerhafte Grundlage

Ein Tool wird umbenannt, eine API wird kostenpflichtig, eine Plattform ändert ihre Profilseiten. Gerade dann zeigt sich, was eine Community leistet: Menschen prüfen Fehlermeldungen, tauschen Erfahrungen aus, schreiben Ersatzlösungen und machen die Änderungen öffentlich nachvollziehbar.

Die Beständigkeit besteht im Weitergeben von Methoden, Datenstrukturen und Korrekturen. Sie beruht auf vielen einzelnen Beiträgen und nicht auf einem einzigen Anbieter. Ein Projekt kann ruhen; eine passende Lizenz und eine nachvollziehbare Dokumentation ermöglichen anderen, seine Arbeit fortzuführen.

Konkrete Formen dieser Zusammenarbeit

- **OSINT Framework:** Beiträge und Korrekturvorschläge ergänzen das gemeinsam gepflegte Ressourcenverzeichnis. [Projekt >](#)
- **WhatsMyName:** Community-Beiträge halten Erkennungsdaten aktuell. Wenn eine Website ihre Antworten ändert, muss die passende Regel berichtigt werden. [Datensatz und Beitragsregeln >](#)
- **Sherlock:** Quellcode und Projektinformationen sind offen einsehbar; die Projektseite nennt Beiträge aus der Gemeinschaft. [Werkzeugprojekt >](#)
- **Bellingcat:** Öffentlich zugängliche Ressourcen und das Toolkit vermitteln Quellen und Arbeitsweisen. [Ressourcen >](#)
- **Trace Labs:** Die Organisation beschreibt die gemeinsame Auswertung offener Informationen zur Unterstützung der Vermisstensuche. Für die Teilnahme gelten ihre jeweiligen Regeln. [Initiative >](#)

Eine begründete Haltung

Unser Angebot steht auf dieser gemeinsamen Arbeit. Wer offene Ressourcen verwendet, sollte Urheber nennen, Lizenzen beachten, Fehler respektvoll melden und nach Möglichkeit etwas zurückgeben. Auch eine gut dokumentierte Korrektur ist ein wertvoller Beitrag.

Beständigkeit braucht Pflege

Offen, kostenlos und ehrenamtlich sind unterschiedliche Eigenschaften. Eine frei erreichbare Website kann kommerziell betrieben werden; freie Software kann externe Bezahlungen benötigen. Ehrenamtliche Arbeit kostet Zeit, und Betreuung kann enden. Eine starke Community verdient Anerkennung und Unterstützung, aber keine unkritische Zuschreibung von Fehlerfreiheit.

Vor der Auswahl eines Projekts helfen erkennbare Verantwortliche, verständliche Dokumentation, nachvollziehbare Änderungen und ein geregelter Umgang mit Fehlern. Sternzahlen oder die Zahl der verlinkten Dienste reichen als Qualitätsnachweis nicht aus. Unsere eigene Verantwortung bleibt bestehen, auch wenn eine Ressource aus der Community stammt.

Wie eine gemeinsame Korrektur aussehen kann

Das folgende Beispiel ist didaktisch, kein Bericht über einen bestimmten Fehlerfall. Es orientiert sich an öffentlich beschriebenen Beitragsabläufen, etwa bei WhatsMyName.

1. **Fehler bemerken:** Ein Checker meldet bei einer Plattform auch für einen nicht vorhandenen Namen einen Treffer.

2. **Ursache eingrenzen:** Die Plattform liefert jetzt eine allgemeine Seite mit HTTP 200. Der Statuscode allein reicht für die Erkennung nicht mehr.
3. **Respektvoll dokumentieren:** Version, Datum und einen nicht personenbezogenen Testfall im vorgesehenen Projektkanal beschreiben. Keine echten Zugangsdaten, vertraulichen Inhalte oder fremden Profile mitsenden.
4. **Gemeinsam prüfen:** Eine passende Erkennungsregel wird vorgeschlagen, geprüft und gegebenenfalls übernommen. Wer die Änderung akzeptiert, hängt von den Projektregeln ab.
5. **Wissen erhalten:** Änderung und Testbedingungen bleiben dokumentiert. Andere Anwendungen können den gepflegten Datensatz weiterverwenden.

Die Community trägt damit über einzelne Oberflächen hinweg Erfahrungen weiter. Das setzt Betreuung, nachvollziehbare Regeln und Rücksicht auf die Zeit der Beteiligten voraus. Eine Fehlermeldung schafft keinen Anspruch auf sofortige Bearbeitung.

[Projektbeschreibung und Beitragsmöglichkeiten >](#)

[Kritischer Gegenpunkt: Werkzeuge können missbraucht werden >](#)

11 · Selbstschutz und Schutz anderer

Eine Recherche kann technische Spuren hinterlassen: Anbieter sehen Anfragen, Logins und je nach Übermittlung Suchbegriffe oder Dateien. VPN, Tor und getrennte Browserprofile bieten unterschiedliche Schutzfunktionen; sie garantieren keine vollständige Anonymität.

Eine getrennte, aktualisierte Arbeitsumgebung hilft, private Konten und Recherche nicht versehentlich zu verbinden. Verschlüsselte Ablage, geregelte Zugriffe und ein Löschantrag sind ebenso wichtig. Zusätzliche Browser-Erweiterungen können neue Risiken und Wiedererkennungsmerkmale schaffen.

Vor einer externen Abfrage

- Was erhält der Anbieter: nur eine öffentliche Domain oder einen vertraulichen Inhalt?
- Ist die Abfrage für die Frage erforderlich und rechtmäßig?
- Gibt es eine lokale Alternative?
- Welche Spuren entstehen für recherchierende und betroffene Personen?

Getrennte Arbeitsidentitäten rechtfertigen keine Täuschung, keine fremde Identitätsübernahme und keinen Zugang zu beschränkten Inhalten. Bei gefährdeten Menschen muss auch bedacht werden, ob schon ein öffentlicher Bericht oder eine Archivierung ihre Lage verschlechtern könnte.

Die Bild- und Hash-Übungen in **Kapitel 13** kommen ohne externe Dateiübermittlung aus.

12 · Von der Beobachtung zur begrenzten Aussage

Analytische Qualität zeigt sich darin, ob die Schlussfolgerung durch das Material getragen wird. Ein Bericht sollte deshalb erkennen lassen, was unmittelbar beobachtet wurde, welche Erklärung erwogen wird und welche Prüfung noch fehlt.

Typische Übergänge, an denen eine Recherche zu weit gehen kann

Beobachtung	Mögliche Erklärung	Gegenprüfung	Damit noch nicht belegt
Zwei Domains zeigen dieselbe IP	Gemeinsamer Betreiber oder gemeinsames Hosting	Zeitraum, Provider und weitere belegte Zuordnungen prüfen	Gemeinsame Urheberschaft
Derselbe Benutzername auf zwei Seiten	Dieselbe Person oder Namensgleichheit	Kontext, Zeitbezug und unabhängige Angaben vergleichen	Identität oder Schuld
Ein älteres Dienst-Banner nennt eine Version	Frühere Installation; eventuell inzwischen aktualisiert	Inventar und freigegebene aktuelle Prüfung	Aktuelle Verwundbarkeit
Ein Dateihash unterscheidet sich	Die verglichenen Bytefolgen unterscheiden sich	Arbeitskopien, Dateiformat und nachvollziehbare Änderung prüfen	Absicht oder Ursache

Mehrere Fundstellen können dieselbe Quelle sein

Drei Nachrichtenportale, die denselben Agenturtext übernehmen, liefern keine drei unabhängigen Bestätigungen. Quellenabhängigkeit gehört deshalb ins Protokoll. Auch zwei tatsächlich unabhängige Quellen können sich irren; eine feste Trefferzahl ist kein Wahrheitsautomat.

Unsicherheit verständlich formulieren

„Hohe Konfidenz“ hilft nur, wenn die Gründe genannt werden. Ohne eine belastbare Kalibrierung sind Prozentzahlen wie „99 Prozent sicher“ irreführend. Besser ist eine begründete Formulierung: „Die beiden unabhängig entstandenen Unterlagen stimmen in Datum und Adresse überein; die heutige Nutzung wurde nicht geprüft.“

Auch die eigene Hypothese prüfen

Wer früh einen Täter vermutet, bewertet passende Fundstellen leicht großzügiger als widersprechende. Halten Sie mindestens eine plausible Alternative fest und suchen Sie gezielt nach einem Befund, der die eigene Annahme schwächen könnte. Bei wichtigen Ergebnissen hilft eine zweite Person, die den Prüfweg unabhängig nachvollzieht.

Die NIST-Handreichung zur Erhaltung digitaler Beweismittel und das Berkeley Protocol geben zusätzliche Orientierung für ihre jeweiligen Anwendungsbereiche. Sie liefern keine automatische Garantie gerichtlicher Verwertbarkeit. [NIST](#) > · [Berkeley Protocol](#) >

[Fehlende und widersprüchliche Ergebnisse einordnen](#) >

13 · Wenn die Recherche nicht weiterführt

Ein leeres Ergebnis ist ebenfalls ein Arbeitsergebnis, wenn die Bedingungen dokumentiert sind. Problematisch wird es, wenn eine technische Grenze als Aussage über die Wirklichkeit ausgegeben wird. Die folgende Übersicht hilft, den nächsten Schritt zu wählen.

Was passiert?	Was daraus folgt	Sinnvoller nächster Schritt
Die Suche liefert keinen Treffer.	Unter diesen Suchbedingungen wurde nichts gefunden. Vollständigkeit ist nicht belegt.	Begriffe, Zeitraum und Abdeckung prüfen; Grenzen im Protokoll nennen.
Die Website verlangt Anmeldung oder sperrt den Abruf.	Die Quelle konnte auf diesem Weg nicht geprüft werden.	Berechtigung und erlaubte Alternativen klären. Zugangssperren nicht umgehen.
Ein Dienst antwortet mit einem Serverfehler.	Der technische Abruf ist derzeit unklar, nicht automatisch dauerhaft unmöglich.	Später angemessen erneut prüfen; Zeitpunkt und Fehlermeldung festhalten.
Im Bild fehlen GPS- oder Zeitfelder.	Die vorliegende Fassung enthält die gesuchten Angaben nicht.	Herkunft und Bearbeitung klären; sichtbaren Kontext gesondert prüfen.
Datumsangaben widersprechen einander.	Möglicherweise werden Ereignis, Veröffentlichung, Archivierung und Abruf verwechselt.	Zeitarten und Zeitzonen getrennt auflisten; offene Widersprüche erhalten.
Eine Seite wurde gelöscht.	Die heute fehlende Seite lässt keinen sicheren Schluss auf früheren Inhalt oder Lösungsgrund zu.	Rechtmäßig zugängliche Archivfassung im zeitlichen Kontext prüfen; Lücken benennen.

Wann ein offenes Ergebnis genügt

Wenn die ursprüngliche Frage beantwortet ist oder der erforderliche weitere Zugriff nicht zulässig beziehungsweise unverhältnismäßig wäre, ist ein dokumentierter Abschluss die richtige Entscheidung. „Mit den verfügbaren Quellen nicht feststellbar“ ist eine fachlich brauchbare Aussage, sofern Methode und Grenzen nachvollziehbar sind.

[Ein vollständig ausgefüllter Musterbericht > · Beobachtung und Schlussfolgerung trennen >](#)

14 · Drei durchgearbeitete Praxisbeispiele

Die Szenarien und Befunde sind fiktiv. `example.com` und die genannten Dateinamen dienen als Platzhalter. Die Beispiele führen keine Abfragen aus und enthalten keine echten Fälle oder personenbezogenen Daten.

Ein echter Fall zum Nacharbeiten

Die öffentliche Startseite dieses Auftritts wurde vor der Umbenennung gesichert und mit der neuen Veröffentlichungsfassung verglichen. Beide HTML-Dateien, SHA-256-Werte, ein ausgefülltes Protokoll und der Musterbericht sind verfügbar.

[Webseitenvergleich nachvollziehen >](#)

Beispiel A · Ein alter Zertifikatsname

Frage: Gibt es einen Hinweis auf ein vergessenes Testsystem in der eigenen, freigegebenen Infrastruktur?

1. Ein vorhandener CT-Auszug nennt `dev.example.com` in einem Zertifikat mit Gültigkeitsbeginn 2021. Auszug und Abrufzeit werden dokumentiert.
2. Eine freigegebene heutige DNS-Prüfung liefert in diesem Szenario keinen passenden Eintrag. In der internen Inventarliste ist der Name als aufgegeben vermerkt.
3. Die Quellen betreffen unterschiedliche Zeitpunkte. Der historische Zertifikatsname bleibt nachvollziehbar, aber er bestätigt keinen heute betriebenen Server.

Begrenztes Ergebnis

„Der Name wurde in einem Zertifikat von 2021 beobachtet. Aktuelle Nutzung wurde mit den genannten Prüfungen nicht bestätigt. Ob zwischenzeitlich ein Dienst existierte, bleibt offen.“

Stoppregel: Nicht nach Backups oder Verwaltungszugängen suchen, nur weil ein früherer Name bekannt ist. Für weitere technische Prüfungen zuerst Umfang und Freigabe klären.

Beispiel B · Das eigene Foto vor der Veröffentlichung

Frage: Enthält mein selbst aufgenommenes Bild unnötige Standort- oder Geräteangaben?

1. Das Original bleibt unverändert. Eine Kopie wird mit ExifTool lokal gelesen, etwa mit dem folgenden Befehl. Er enthält keine Schreiboption und lädt nichts hoch.
2. Gefundene Felder werden dokumentiert: Feldname, Wert und Dateifassung. Ein Aufnahmezeitfeld kann eine Gerätezeit ohne eindeutige Zeitzone enthalten.
3. Für die Veröffentlichung wird eine gesonderte Fassung erstellt. Danach wird diese erneut geprüft; bei einem echten Beweisstück ist eine solche Veränderung nicht der richtige erste Schritt.

```
exiftool -G1 -s eigenes-bild.jpg
```

Begrenztes Ergebnis

„In der untersuchten Fassung wurden GPS-Felder gefunden. Ihre Richtigkeit wurde nicht unabhängig bestätigt. In der Veröffentlichungsfassung sind diese Felder beim erneuten Lesen nicht mehr sichtbar.“

Grenze: Die Prüfung sämtlicher anderer Metadaten und sichtbarer Standortmerkmale ist damit nicht abgeschlossen. Ein Straßenschild im Bild kann mehr verraten als ein GPS-Feld.

Beispiel C · Zwei rechtmäßig vorhandene PDF-Fassungen

Frage: Sind die beiden erhaltenen Dateien bytegleich, und wo unterscheiden sich ihre Texte?

1. Dateinamen, Herkunft, Erhaltzeit und Arbeitskopien werden notiert. Die Originale werden nicht überschrieben.
2. Die SHA-256-Werte werden lokal ermittelt, etwa in PowerShell. Die Befehle lesen die Dateien, ohne sie an einen Dienst zu senden.
3. Unterschiedliche Hashwerte belegen unterschiedliche Bytefolgen. Anschließend werden die Texte an Arbeitskopien verglichen. Eine reine Metadatenänderung kann den Hash ebenfalls verändern.

```
Get-FileHash -LiteralPath .\fassung-a.pdf -Algorithm SHA256  
Get-FileHash -LiteralPath .\fassung-b.pdf -Algorithm SHA256
```

Begrenztes Ergebnis

„Die Dateien sind nicht bytegleich. Im Textvergleich unterscheidet sich Absatz 3. Ursache, Urheberschaft und Zeitpunkt der Änderung wurden nicht festgestellt.“

Grenze: Ein Hash bestätigt weder die behauptete Herkunft einer Datei noch den Wahrheitsgehalt ihres Inhalts. Dieses Beispiel betrifft lokale Dokumentenprüfung und ist kein reiner OSINT-Fall.

[Rechercheprotokoll herunterladen >](#) · [SHA-256 im lokalen Browser-Werkzeug prüfen >](#)

15 · KI und Automation mit überprüfbarem Nutzen

Automation kann Fundstellen ordnen, Dubletten kennzeichnen und wiederkehrende Abfragen vereinfachen. Ob sie eine Recherche verbessert, lässt sich an weniger manueller Nacharbeit, nachvollziehbaren Fehlern und der Qualität des Ergebnisses prüfen. Pauschale Zeitersparnisse oder feste „Fehlerquoten“ sind ohne Messgrundlage kein belastbares Argument.

Ein sinnvoll begrenzter KI-Einsatz

Bei zwei öffentlichen Textfassungen kann ein Sprachmodell Änderungsvorschläge für eine Vergleichsliste liefern. Jede aufgeführte Änderung muss anschließend in den tatsächlichen Fassungen nachgesehen werden. Die Liste wird als Entwurf behandelt; Modell, Version und übermittelte Inhalte gehören zur Dokumentation.

KI kann Quellen erfinden, eine Aussage verstärken oder unsichere Identitätsverbindungen überzeugend formulieren. Eine verständliche Antwort ist daher noch kein geprüfter Befund. Bei vertraulichen Unterlagen ist zusätzlich zu klären, ob und an welchen Anbieter sie übermittelt werden dürfen.

Herkunftsdaten richtig einordnen

C2PA beschreibt technische Verfahren für signierte Angaben zur Herkunft und Bearbeitung von Medien. Solche Angaben können eine Prüfung unterstützen. Sie beweisen nicht automatisch die Wahrheit einer dargestellten Szene; ihr Fehlen macht ein Bild nicht zur Fälschung. [Initiative und Spezifikation >](#)

Unser Maßstab

KI ist dort hilfreich, wo ihr Beitrag überprüfbar bleibt. Die Verantwortung für Auswahl, Gegenprüfung und Veröffentlichung lässt sich nicht an ein Modell abgeben. Offene Community-Arbeit kann auch hier Methoden und Fehler transparent machen.

16 · Glossar und nachprüfbare Quellen

OSINT

Methodische Auswertung rechtmäßig zugänglicher offener Informationen für eine festgelegte Frage.

Pivot

Übergang von einer Information zu einer möglichen weiteren Verbindung, die gesondert geprüft werden muss.

IOC

Indicator of Compromise: technischer Hinweis auf einen möglichen Sicherheitsvorfall, kein alleiniger Nachweis.

Provenienz

Herkunft und nachvollziehbare Verarbeitung eines Informationsobjekts.

Konfidenz

Begründete Einschätzung der Belastbarkeit einer Aussage; ohne Kalibrierung keine Prozentwahrscheinlichkeit.

RDAP

Registration Data Access Protocol: standardisierter Zugang zu Domain-Registrierungsdaten.

CT

Certificate Transparency: öffentliche Protokolle zu Zertifikaten.

OpSec

Operations Security: Maßnahmen zur Begrenzung von Risiken für die Recherche und betroffene Menschen.

Projekt-, Anbieter- und Primärquellen

Die folgenden Links führen zu Projekten, Anbietern oder den Herausgebern der genannten Dokumente. Der Quellenabgleich und die technische Verweisprüfung sind unterschiedliche Prüfungen. Ein erfolgreicher Abruf bestätigt keine vollständige Funktion oder Sicherheit eines Angebots.

- **OSINT Framework: Projekt, Legende und Mitwirkung** Verweisprüfung 12.10.2026: HTTP erreichbar (HTTP 200)
- **WhatsMyName: Community-Datensatz und Beitragsregeln** Verweisprüfung 12.10.2026: HTTP erreichbar (HTTP 200)
- **Sherlock: Projektbeschreibung und Dokumentation** Verweisprüfung 12.10.2026: HTTP erreichbar (HTTP 200)
- **Bellingcat: öffentliche Ressourcen** Verweisprüfung 12.10.2026: HTTP erreichbar (HTTP 200)
- **Bellingcat Toolkit: Werkzeugverzeichnis** Verweisprüfung 12.10.2026: HTTP erreichbar (HTTP 200)
- **Trace Labs: Initiative zur Vermisstensuche** Verweisprüfung 12.10.2026: Abruf geschützt/begrenzt - manuell prüfen (HTTP 403)
- **theHarvester: Projekt und Einsatzgrenzen** Verweisprüfung 12.10.2026: HTTP erreichbar (HTTP 200)
- **SpiderFoot: Projekt und Module** Verweisprüfung 12.10.2026: HTTP erreichbar (HTTP 200)
- **Maltego: Anbieter und Produktinformationen** Verweisprüfung 12.10.2026: HTTP erreichbar (HTTP 200)
- **Gephi: offene Graph-Visualisierung** Verweisprüfung 12.10.2026: HTTP erreichbar (HTTP 200)

- **Shodan: technische Suchmaschine** Verweisprüfung 12.10.2026: HTTP erreichbar (HTTP 200)
- **Censys: Anbieter und technische Recherche** Verweisprüfung 12.10.2026: HTTP erreichbar (HTTP 200)
- **crt.sh: Zertifikatsrecherche** Verweisprüfung 12.10.2026: Automatischer Abruf unklar (HTTP 502)
- **ICANN: Registration Data Access Protocol** Verweisprüfung 12.10.2026: HTTP erreichbar (HTTP 200)
- **Have I Been Pwned: Grenzen und Funktionsweise in den FAQ** Verweisprüfung 12.10.2026: HTTP erreichbar (HTTP 200)
- **ExifTool: Originalprojekt und Dokumentation** Verweisprüfung 12.10.2026: HTTP erreichbar (HTTP 200)
- **NIST IR 8387: Erhaltung digitaler Beweismittel** Verweisprüfung 12.10.2026: HTTP erreichbar (HTTP 200)
- **Berkeley Protocol: vollständiges Dokument beim Mitherausgeber (PDF)** Verweisprüfung 12.10.2026: HTTP erreichbar (HTTP 200)
- **DSGVO: offizieller Rechtstext** Verweisprüfung 12.10.2026: HTTP erreichbar (HTTP 202)
- **Österreich: § 118a StGB im RIS** Verweisprüfung 12.10.2026: HTTP erreichbar (HTTP 200)
- **C2PA: Herkunfts- und Bearbeitungsangaben zu Medien** Verweisprüfung 12.10.2026: HTTP erreichbar (HTTP 200)

Redaktioneller Quellenabgleich: 12. Oktober 2026. Das Prüfprotokoll enthält 28 unterschiedliche externe Verweise, einschließlich Lizenz und kommentierter Fachlektüre. Die technischen Abrufe sind Momentaufnahmen; erfolgreiche HTTP-Antworten bestätigen keine vollständige Funktion, Aktualität oder Sicherheit. [Prüfprotokoll herunterladen](#)

[Aufnahme- und Review-Kriterien >](#) · [Korrektur oder Anregung zum Webangebot mitteilen >](#)

Deutschsprachig weiterlesen - mit redaktioneller Einordnung

Die Auswahl ergänzt Projektseiten um journalistische und pädagogische Arbeitsweisen. Hier stehen kurze eigene Einordnungen; die Originaltexte bleiben bei ihren Herausgebern. Ein älterer Beitrag kann methodisch wertvoll sein und zugleich überholte Bedienhinweise enthalten. Alle folgenden Verweise wurden am 12. Oktober 2026 redaktionell betrachtet.

APA · Regeln des Faktenchecks

Österreich · Grundlagenseite, mit im Text erläuterten Regeländerungen · Abruf 12.10.2026

Hilft bei: dem Aufbau eines nachvollziehbaren Ergebnisses. Die APA beschreibt transparente Verifizierung, Gegenbelege und eine zusätzliche redaktionelle Prüfung.

Unsere Einordnung: Ein gutes Vorbild für einen Musterbericht. Die Regeln einer Nachrichtenagentur ersetzen keine forensische Verfahrensvorschrift. Das dort beschriebene Vier-Augen-Prinzip wurde für diesen Leitfaden noch nicht durch eine unabhängige fachkundige Person umgesetzt.

[Originalbeitrag lesen](#)

Technische Verweisprüfung 12.10.2026: HTTP erreichbar (HTTP 200)

Saferinternet.at · Onlineinhalte überprüfen

Österreich · Informationskompetenz, insbesondere für Kinder, Jugendliche und Lehrende · Abruf 12.10.2026

Hilft bei: Quellenvergleich, Bildkontext und dem kritischen Umgang mit vermeintlich plausiblen Inhalten.

Unsere Einordnung: Verständlicher Einstieg auch für Erwachsene. Ein pädagogischer Überblick ist keine vollständige Bildforensik; automatische Erkennungsmerkmale allein entscheiden nicht über Echtheit.

[Originalbeitrag lesen](#)

Technische Verweisprüfung 12.10.2026: HTTP erreichbar (HTTP 200)

CORRECTIV · Bilderrückwärtssuche

Deutschland · 1. April 2022 · Abruf 12.10.2026

Hilft bei: dem Vergleich einer verbreiteten Aufnahme mit anderen Veröffentlichungen. Der Beitrag führt einen konkreten Bildvergleich vor.

Unsere Einordnung: Gut zum Verständnis der Methode. Oberflächen und mobile Funktionen haben sich seit 2022 verändert. Vor jeder externen Bildübermittlung bleiben Berechtigung und Vertraulichkeit zu prüfen.

[Originalbeitrag lesen](#)

Technische Verweisprüfung 12.10.2026: HTTP erreichbar (HTTP 200)

CORRECTIV · Recherche-Tricks für Suchmaschinen

Deutschland · 11. März 2023 · Abruf 12.10.2026

Hilft bei: der bewussten Eingrenzung von Suchanfragen, Dokumenttypen und Zeiträumen.

Aktualisierungshinweis: Der Beitrag empfiehlt noch `cache:`. Dieser Operator funktioniert laut Googles Dokumentationsänderung vom September 2024 nicht mehr. Auch andere Bedien- und Operatorhinweise sollten vor der Anwendung gegen die aktuelle Anbieterhilfe geprüft werden.

[Originalbeitrag lesen](#)

Technische Verweisprüfung 12.10.2026: HTTP erreichbar (HTTP 200)

Bellingcat · Missbrauch digitaler Recherchertools

Deutschsprachiger Beitrag von Johanna Wild · 24. November 2021 · Abruf 12.10.2026

Hilft bei: dem Erkennen von Logiksprüngen. Die Recherche beschreibt, wie Karten und andere offene Werkzeuge für unbelegte Deutungen in QAnon-Kontexten verwendet wurden.

Unsere Einordnung: Ein notwendiger Gegenpunkt zur Werkzeugbegeisterung. Öffentlich verfügbare Daten und gemeinschaftliche Arbeit sichern die Qualität nicht von selbst. Jede konkrete Verknüpfung braucht eine tragfähige Begründung; eine unterstellte Absicht ist kein Beweis.

[Originalbeitrag lesen](#)

Technische Verweisprüfung 12.10.2026: HTTP erreichbar (HTTP 200)

Google · Änderungen an der Suchdokumentation

Offizielle Anbieterquelle · deutsche Sprachansicht · Eintrag vom September 2024

Hilft bei: dem Gegenprüfen älterer Suchanleitungen. Der Änderungsverlauf erläutert die Entfernung der Dokumentation zum nicht mehr funktionierenden `cache:-`Operator.

Unsere Einordnung: Für konkrete Anbieterfunktionen ist die aktuelle Originaldokumentation maßgeblich. Ihre technische Aussage ist trotzdem kein Nachweis, dass Suchergebnisse vollständig sind.

Originaldokumentation lesen

Technische Verweisprüfung 12.10.2026: HTTP erreichbar (HTTP 200)

Redaktioneller Prüfstand

Stand: 12. Oktober 2026. Inhalte, interne Verweise und ausgewählte Quellen wurden redaktionell geprüft; der eigene Webseitenvergleich wurde technisch nachgerechnet. Eine unabhängige fachliche Gegenlese durch eine weitere qualifizierte Person steht noch aus. Die redaktionelle Überarbeitung wird nicht als Zertifizierung oder unabhängiges Fachgutachten bezeichnet.

[Sachliche Korrektur oder Anregung zum Angebot mitteilen >](#)

Autor und Lizenz

Praxisleitfaden: Thomas Lechleitner, MSc · Seitenbetreiber. Redaktionell überarbeitete Webfassung, 12. Oktober 2026. Lizenz: [CC BY-NC-SA 4.0](#) . Rechte an verlinkten Drittinhalten bleiben unberührt.

[Zum Anfang](#)

Quellenadressen zum Nachlesen

Diese Liste führt die im Kompass verlinkten externen Quellen zusammen. Technische Erreichbarkeit und inhaltliche Prüfung sind unterschiedliche Dinge. Prüfstände und Einschränkungen finden Sie im Quellenteil des Leitfadens.

1. <https://github.com/lockfale/OSINT-Framework>
2. <https://github.com/WebBreacher/WhatsMyName>
3. <https://github.com/sherlock-project/sherlock>
4. <https://www.bellingcat.com/resources/>
5. <https://bellingcat.gitbook.io/toolkit/>
6. <https://tracelabs.org/>
7. <https://github.com/laramies/theHarvester>
8. <https://github.com/smicallef/spiderfoot>
9. <https://www.maltego.com/>
10. <https://gephi.org/>
11. <https://www.shodan.io/>
12. <https://censys.com/>
13. <https://crt.sh/>
14. <https://www.icann.org/en/contracted-parties/registry-operators/resources/registration-data-access-protocol>
15. <https://haveibeenpwned.com/FAQs>
16. <https://exiftool.org/>
17. <https://www.nist.gov/publications/digital-evidence-preservation-considerations-evidence-handlers>
18. <https://humanrights.berkeley.edu/wp-content/uploads/archive/2024/02/Berkeley-Protocol.pdf>
19. <https://eur-lex.europa.eu/eli/reg/2016/679/oj/deu>
20. <https://www.ris.bka.gv.at/NormDokument.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296&Paragraf=118a>
21. <https://c2pa.org/>
22. <https://apa.at/faktencheck/regeln/>
23. <https://www.saferinternet.at/wie-ueberprueft-man-onlineinhalte>
24. <https://correctiv.org/faktencheck/hintergrund/2022/04/01/so-funktioniert-die-bilderrueckwaertssuche/>
25. <https://correctiv.org/faktencheck/faktencheck-tipps/2023/03/11/einfache-suchmaschinen-tricks-auf-google/>
26. <https://de.bellingcat.com/nachrichten/2021/11/24/flight-tracking-seiten-satellitenbilder-und-google-maps-wie-qanon-anhanger-digitale-recherchetools-missbrauchen/>
27. <https://developers.google.com/search/updates?hl=de#cache-docs>
28. <https://creativecommons.org/licenses/by-nc-sa/4.0/>