

OSINT

Wie Sie Informationen finden, verifizieren und verknüpfen

» Hier geht's
direkt
zum Buch

DIE LESEPROBE

einem Jahr ganz anders aussehen als heutige Prototypen. Richtig umgesetzt, wäre ein solcher *Agent* Ihr ständiger Begleiter, den sie sowohl für die anfängliche Recherche als auch für die laufende Überwachung von Informationsquellen und Entwicklungen einsetzen können.

7.1.2 Suchstrategie

Im nächsten Abschnitt erhalten Sie wertvolle Tipps, mit denen Sie Ihre Suche effizient und systematisch gestalten können.

Suchbegriffe und Themen

Alles beginnt mit einer Auswahl geeigneter Suchbegriffe. Starten Sie mit allgemeinen Begriffen und konkretisieren Sie diese im Verlauf Ihrer Recherche. Die Identifikation von primären und sekundären Keywords hilft, verschiedene Aspekte eines Themas abzudecken. Dabei ist die gezielte Suche nach *Entitäten* (also Personen, Organisationen, Orten oder Ereignissen) notwendig, um konkrete Ergebnisse zu erzielen.

Die *Keyword-Recherche* bildet das Fundament jeder erfolgreichen Suchstrategie. Überlegen Sie, welche Begriffe Ihr Thema am besten beschreiben, und nutzen Sie Synonyme sowie verwandte Ausdrücke. Berücksichtigen Sie dabei die Zielgruppe sowie den Kontext der Informationssuche.

Primäre Keywords sind die zentralen Schlagwörter, die Ihre Suche widerspiegeln. Sekundäre Keywords dienen dazu, die Suche oder den Kontext zu erweitern.

Durch die Kombination von mehreren Entitäten in einer Suchanfrage können Beziehungen und Zusammenhänge zwischen ihnen aufgedeckt werden.

Successive Fractions Approach

Der *Successive Fractions Approach* ist eine Methode zur schrittweisen Eingrenzung der Suchtreffer und folgt dem genannten Grundsatz »vom Allgemeinen zum Speziellen«. Beim Successive Fractions Approach starten Sie mit einer breiten Suche, um so einen ersten Überblick über das Thema bzw. die Suchergebnisse zu erhalten. Im nächsten Schritt fügen Sie erste Filter hinzu, um relevante Unterkategorien zu identifizieren und irrelevante Treffer zu entfernen. Mit weiteren Filtern und Ausschlüssen verfeinern Sie Ihre Suche so lange, bis Sie eine handhabbare Menge an Suchtreffern erreicht haben.

Gibt es bestimmte Zeiträume, Orte oder Eigenschaften, auf die Sie die Suche eingrenzen können? Indem Sie solche Details in Ihre Suchanfrage integrieren, verringern Sie die Anzahl der Suchergebnisse immer weiter.

Boolesche Operatoren

Logische Verknüpfungen, auch als *boolesche Operatoren* bekannt, dienen dazu, mehrere Suchbegriffe oder Eigenschaften zu kombinieren. Zwei Suchbedingungen können grundsätzlich über die Operatoren *OR*, *AND* oder *NOT* verknüpft werden (in Abschnitt 7.2.3 erläutere ich das an einem konkreten Beispiel).

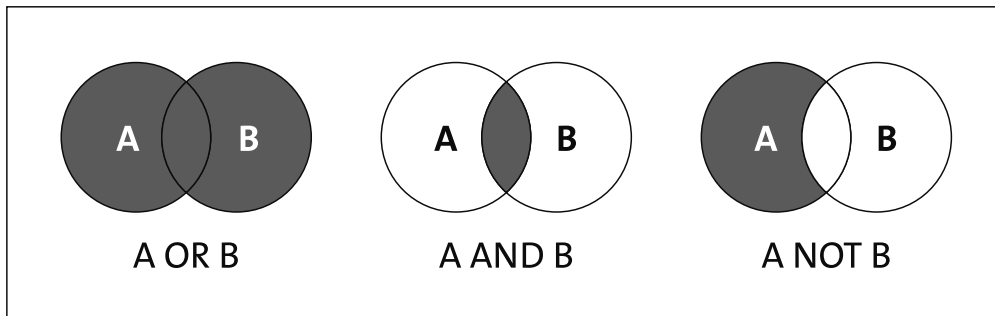


Abbildung 7.1 Logische Verknüpfungen

- ▶ Das logische *Oder* (*OR*) liefert Ergebnisse, die entweder einen der ausgewählten Begriffe oder beide enthalten. In bestimmten Fällen kann das XOR verwendet werden, um Ergebnisse auszuschließen, die beide Suchbegriffe gemeinsam aufweisen. Diese Option ist jedoch selten verfügbar.
- ▶ Das logische *Und* (*AND*) erfordert, dass beide Bedingungen erfüllt sind, sodass nur die Schnittmenge der Ergebnisse ausgegeben wird.
- ▶ Beim logischen *Ausschluss* (*NOT*) werden alle Ergebnisse zum ersten Suchbegriff angezeigt, wobei diejenigen ausgeschlossen werden, bei denen auch die zweite Bedingung zutrifft.

Kontextualisierung

Ein weiterer wichtiger Aspekt ist die Kontextualisierung der Suche. Überlegen Sie, ob Sie einen Kontext ergänzen können. Bei der Suche nach einer Person kann das Hinzufügen von Hobbys oder anderen Eigenschaften den Unterschied machen, ob Sie fündig werden oder nicht – insbesondere dann, wenn diese Person einen häufig vorkommenden Namen hat. Durch das Hinzufügen von Kontextbegriffen können Sie die Suchergebnisse verfeinern und so gezielt Fachbeiträge, Nachrichtenartikel oder Studien finden, die genau Ihre Fragestellung adressieren.

Varianten und Wildcards

Um Ihre Suchergebnisse weiter zu optimieren, sollten Sie auch sprachliche Variationen der Suchwörter berücksichtigen. Dazu gehört beispielsweise auch, den Suchbegriff in anderen Sprachen in Ihre Recherche einzubeziehen – etwa bei internationalen Themenbereichen oder dann, wenn relevante Informationen in anderen Landessprachen vermutet werden.

Trunkierung, also das Abschneiden von Wortstämmen, kann helfen, unterschiedliche Wortendungen oder -formen zu erfassen, z. B. Comput* für Computer, Computing, Computersystem. Auch das bewusste Auflösen von Abkürzungen ist sinnvoll, da Begriffe sowohl ausgeschrieben als auch abgekürzt auftauchen können. Außerdem besteht bei Abkürzungen immer die Gefahr, dass diese mehrere Bedeutungen haben können. Unterschiedliche Schreibweisen wie z. B. E-Mail, Email oder eMail sollten einbezogen werden, um keine relevanten Ergebnisse zu versäumen.

Bei vielen Suchen besteht die Option, Platzhalter in Form sogenannter *Wildcard*s einzusetzen. Das sind nützliche Werkzeuge, um Unklarheiten in der Schreibweise auszugleichen oder um verschiedene Varianten eines Begriffs in einer Suchanfrage abzudecken. Häufig kann ein Fragezeichen (?) beispielsweise für ein Zeichen oder ein Asterisk (*) als Platzhalter für beliebige Zeichenfolgen dienen, z. B. Organisat* für Organisation oder Organisator.

Slang und Emojis

In manchen Fällen lohnt es sich, nach Slang, Szenesprache oder sogar Emojis zu suchen, da vor allem in sozialen Netzwerken oder Foren Informationen in anderen Ausdrucksformen geteilt werden. Hier zeigt sich, dass zusätzlich zur Recherchemethodik spezifisches Fachwissen – beispielsweise für einen konkreten Deliktsbereich – erforderlich ist, um effizient zu recherchieren.

Diversifizierung der Quellen

Sie werden in diesem Buch an vielen Stellen lesen, dass Sie Ergebnisse verifizieren müssen, indem Sie mehrere Quellen zurate ziehen. Doch tatsächlich sollten Sie bereits bei der Suche mehrere Quellen verwenden. Dies hat vielerlei Gründe.

- ▶ Erstens hat jede Quelle einen begrenzten Suchraum. Unter Umständen liegt das relevante Ergebnis außerhalb des Suchraums der einen, aber innerhalb des Suchraums einer anderen Suchmaschine. Nutzen Sie mehrere Quellen, dann durchsuchen Sie einen größeren Suchraum und finden folglich mehr Treffer.
- ▶ Zweitens sorgen Sie so für Redundanz und Ausfallsicherheit. Sollte eine Quelle (temporär) nicht mehr funktionieren, können Sie ohne Umstände auf eine andere Quelle ausweichen.
- ▶ Drittens wirkt Quellenvielfalt sogenannten Filterblasen entgegen. Auch können Sie durch den Zugriff auf verschiedene Quellen geografische Zensur umgehen. Im Übrigen variieren Suchergebnisse je nach vermutetem Standort und den Spracheinstellungen des Endgeräts.

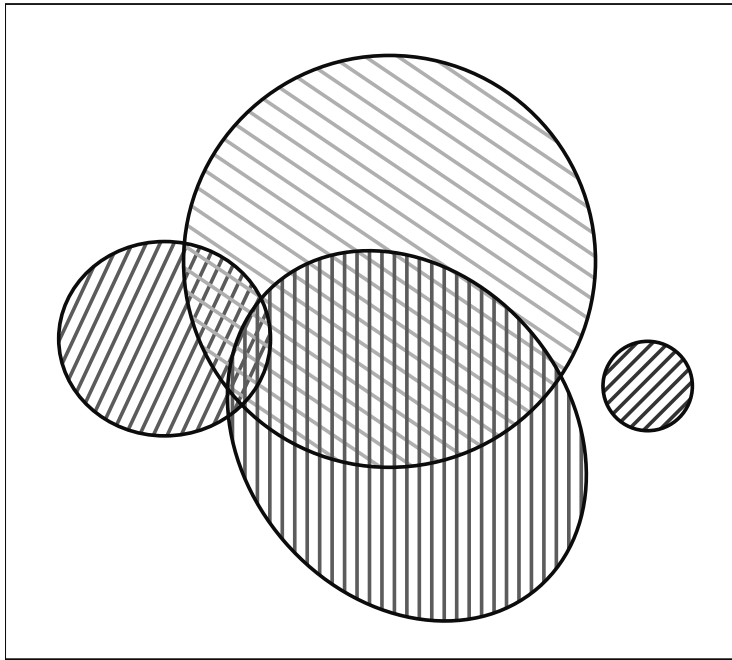


Abbildung 7.2 Überlappende Suchräume

Keyword-Matrix

Mit einer *Keyword-Matrix* können Sie noch strukturierter vorgehen. Erstellen Sie hierfür eine Tabelle, in der Sie zunächst sämtliche relevanten Suchbegriffe in einer Zeile erfassen. Im nächsten Schritt fügen Sie für jeden Begriff Variationen hinzu, beispielsweise unterschiedliche Schreibweisen, Übersetzungen in andere Sprachen, Synonyme, Abkürzungen oder Szenebegriffe. So erhalten Sie eine Übersicht, mit der Sie gezielt komplexe Suchanfragen konstruieren können.

Die Keyword-Matrix ist insbesondere bei umfangreichen Recherchen, die über einen längeren Zeitraum geführt werden, sowie bei der Teamarbeit ein äußerst hilfreiches Werkzeug. Sie unterstützt dabei, eine Vielzahl von Suchbegriffen und deren Kombinationen systematisch zu erfassen, zu dokumentieren und strategisch abzuarbeiten. Rechercheprozesse werden so nachvollziehbar strukturiert und können bei Bedarf gezielt erweitert oder angepasst werden.

Suchbegriff	<i>Blankokarten</i>	...
Oberthema	<i>Kreditkartenbetrug</i>	
Synonym	<i>PVC-Karten</i>	
Andere Sprachen	<i>EN: plastic card</i> <i>ES: tarjeta de plástico</i>	
Szenebegriff	<i>white plastics</i>	

Tabelle 7.1 Keyword-Matrix

Keywords mit KI erstellen

Künstliche Intelligenz (KI) kann die Erstellung einer Keyword-Matrix vereinfachen und beschleunigen. Passende Anwendungen können etwa aus einem vorgegebenen Set an Schlüsselbegriffen automatisch weitere relevante Keywords generieren. Zusätzlich erkennen sie semantische Zusammenhänge und schlagen weitere Begriffe vor, was Ihre Recherche umfassender macht. Abbildung 7.3 zeigt ein Beispiel von ChatGPT.

Suchbegriff (DE)	Oberthema	Synonyme / Slang (DE)	EN	ES	FR	RU	Typische Emojis / Symbolik
Koks	Kokain	Schnee, Nase, Puder	coke, blow, white	perico, blanca	poudre, coke	кокс	🧊👃👉👎
Kokain	Kokain	Stoff, Schnee, weißes	cocaine	cocaína	cocaïne	кокаин	🧊👉👎
Gras	Cannabis	Weed, Ganja, Zeug	weed, grass	verde, maría	beuh, herbe	трава	🌿👃👉👎
Cannabis	Cannabis	Gras, Hasch, Dope	cannabis, pot	marihuana, hierba	cannabis, beuh	каннабис	🌿👃👉👎
Haschisch	Cannabis	Hasch, Platte, Piece	hash, resin	costo, hachís	hasch, résine	гашиш	👃👉👎
MDMA	MDMA / Ecstasy	Tabletten, Pillen, Molly	molly, ecstasy	éxtasis	ecsta, cachet	экстази	👉👎👃👉👎
Ecstasy	MDMA / Ecstasy	Bunte, XTC, Herzchen	ecstasy, pill	pastilla	cachet	экстази	👉👎👃👉👎
Speed	Amphetamin	Pepp, Pepp, Base	speed, amphetamine	anfeta	speed	амфетамин	👉👎👃👉👎

Abbildung 7.3 Erstellung einer Keyword-Matrix mithilfe von ChatGPT

Ein weiterer Vorteil besteht darin, dass KI-Systeme große Datenmengen aus unterschiedlichen Quellen analysieren und daraus Muster für Ihre Recherche ableiten können. Richtig eingesetzt, helfen sie bei der Priorisierung von Suchbegriffen, etwa nach Relevanz oder Häufigkeit im Kontext des jeweiligen Oberthemas.

Am besten funktioniert die Erstellung mithilfe von KI, wenn Sie möglichst konkret vorgeben, welche Inhalte die Matrix abdecken soll, und ein Set von Keywords als Ausgangsbasis zur Verfügung stellen.

Gerade im Team sorgt eine Keyword-Matrix für Transparenz. Erweitert man die Matrix um Spalten für durchgeführte Suchen, können alle jederzeit sehen, wo noch Fragen offen sind. Die Matrix dient zudem als Dokumentationsgrundlage, um später nachzuvollziehen, welche Suchen unternommen wurden. Dies kann Ihnen helfen, wenn Sie belegen müssen, dass Sie auch andere Ermittlungsansätze verfolgt haben.

Auch für die Übergabe einer Recherche an andere Teammitglieder ist eine gepflegte Keyword-Matrix von großem Vorteil, da sie den Wissenstransfer erleichtert. Dies macht insbesondere bei auf Dauer angelegten Recherchen Sinn, beispielsweise bei der Beobachtung eines Phänomenbereichs. Gleichzeitig erleichtert es den Einstieg in die Thematik.

JavaScript: Logik und Interaktion

JavaScript ist die Programmiersprache des Webs. Sie definiert das Verhalten von Webseiten und macht diese interaktiv. Tatsächlich wird JavaScript heutzutage sogar zur Entwicklung ganzer Webanwendungen eingesetzt. Typische Einsatzbereiche sind:

- ▶ Validierung von Formulareingaben
- ▶ dynamische Manipulation des DOM
- ▶ asynchrone Datenübertragung
- ▶ Steuerung von Animationen, Menüs oder Benutzerinteraktionen

Document Object Model

Das *Document Object Model (DOM)* ist die interne Datenstruktur, mit der der Browser eine Webseite darstellt. Es bildet die HTML-Struktur als Baumdiagramm ab, in dem jedes Element ein Node (Knoten) ist. JavaScript und andere Skriptsprachen können auf diese Knoten zugreifen, sie verändern oder dynamisch neue Elemente einfügen.

Dank JavaScript können Webseiten auf Nutzeraktionen reagieren, Daten nachladen oder Inhalte dynamisch anpassen, ohne die Seite vollständig neu laden zu müssen.

JavaScript-Bookmarklets

JavaScript-Bookmarklets sind kleine JavaScript-Programme, die als Browser-Lesezeichen (Bookmarks) gespeichert werden. Statt zu einer Webseite zu navigieren, führen sie beim Anklicken JavaScript-Code direkt im Kontext der aktuell geladenen Webseite aus. Dadurch können sie die Seite dynamisch verändern, Daten extrahieren, Formulare automatisieren oder andere wiederkehrende Aufgaben vereinfachen, ohne dass Erweiterungen installiert werden müssen.

Eine wachsende Sammlung OSINT-spezifischer Bookmarklets, z. B. zur Extraktion der User-ID eines Instagram-Accounts, finden Sie unter <https://tools.myosint.training>.

7.11.4 Ermittlungen zu URLs

In URLs stecken viele Informationen. Manche davon sind nicht immer offensichtlich. Genau deshalb ist das Tool *unfurl* Gold wert.

Das Online-Tool, das Sie unter <https://dfir.blog/unfurl/> finden, bereitet die eingegebene URL grafisch auf und zerlegt sie in ihre einzelnen Bestandteile. Darüber hinaus werden die Bestandteile um weitere Informationen angereichert oder Daten decodiert, um diese verständlich zu machen. Beispielsweise werden bekannte Domains als solche gekennzeichnet oder Zeitstempel in ein menschenlesbares Format umgewandelt. So können Sie bereits anhand der URL den Zeitpunkt eines Social-Media-Beitrags erkennen.

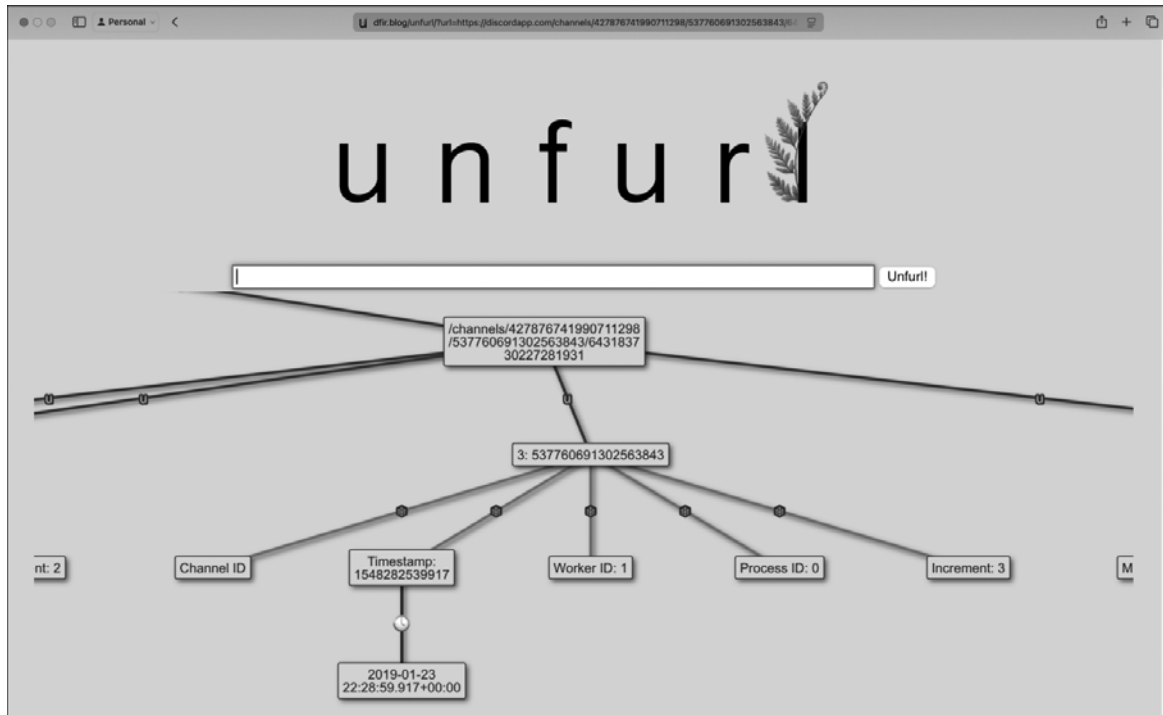


Abbildung 7.104 »unfurl« löst einen Discord-Zeitstempel auf

Es gibt weitere nützliche Online-Tools im Kontext der OSINT-Analyse von URLs und Webdaten. Zum Beispiel *unshorten.it* (<https://unshorten.it>), ein praktisches Tool, um verkürzte URLs (Short-URLs) zu entschlüsseln und die Originaladresse sichtbar zu machen. Es hilft dabei, potenziell versteckte oder verschleierte Ziele hinter Kurzlinks nachvollziehbar zu machen.

Die Suchplattform GrayhatWarfare Shortener Search (<https://shorteners.grayhatwarfare.com/shorteners>) durchsucht systematisch URL-Shortener-Services wie *TinyURL* oder *bit.ly*, um kürzlich oder aktiv genutzte Kurzlinks und deren vollständige Zieladressen zu finden. Das Tool nutzt unter anderem Bruteforce-Methoden, um den kleineren URL-Raum von Shortenern abzudecken, und filtert dabei inaktive oder ungültige Links heraus. So lassen sich oft verborgene oder schwer auffindbare Webressourcen ausfindig machen, darunter auch sensible Dateien in Cloud-Diensten.

Der *Backlink Checker* von *Ahrefs* (<https://ahrefs.com/backlink-checker>) ist ein umfangreiches SEO-Tool zur Untersuchung von Backlinks und Linkprofilen einer Domain oder URL. Es bietet Einblicke in verweisende Domains, Domain-Ratings und organischen Traffic.

7.11.5 Ermittlungen zu Webseiten

Die Ermittlungsansätze zu Webseiten können in thematische Cluster unterteilt werden, um eine strukturierte Herangehensweise zu gewährleisten:

1. Domain- und Inhaberinformationen
2. Infrastruktur und technische Umsetzung
3. Inhaltsanalyse
4. Verbindungen und Verweise
5. Verhalten und Reputation

Domains finden

Sollten Sie noch keine relevante Domain für Ihre Recherche identifiziert haben, dann möchte ich Ihnen zusätzlich zu den bereits behandelten Recherchemöglichkeiten über Suchmaschinen oder in sozialen Netzwerken einige weitere Optionen vorstellen.

Sollten Sie nur eine oder wenige Domains auf deren Existenz prüfen wollen, dann können Sie mit den Befehlszeilentools `nslookup` (Windows) bzw. `dig` (Linux/macOS) feststellen, ob dem gesuchten Domainnamen eine IP-Adresse zugeordnet werden kann.

Die Firma *Netcraft* stellt unter <https://searchdns.netcraft.com> eine Abfragemaske zur Verfügung, mit der Domains anhand ihrer Bestandteile gefunden werden können. Bemerkenswert ist die Suchsyntax, die auch Suchen nach Mustern zulässt. Leider basieren die Ergebnisse nur auf den Seiten, die von Nutzern der Netcraft-Browser-Erweiterung aufgerufen wurden.

Eine ähnliche Möglichkeit bietet die Keyword-Suche von *Whoxy*. Wenn Sie die Website unter <https://whoxy.com> aufrufen, können Sie neben dem Suchfeld über das Dropdown-Menü den Punkt `DOMAIN KEYWORD` auswählen. Sie erhalten dann Ergebnisse von Domains, die das eingegebene Keyword enthalten. Da es sich um einen Freemium-Anbieter handelt, sind die kostenlosen Treffer auf maximal 1.000 beschränkt. Zum Vergleich: Der Anbieter *DNSlytics* limitiert die Ergebnisse auf 50 Treffer.

Darüber hinaus bietet *DNSTwist* (<https://dnstwist.it>) eine Spezialsuche, die Domains mit potenziellen Tippfehlern (*Typo-Squatting*) oder Varianten erzeugt und überprüft. Dieses Tool hilft insbesondere dabei, gefälschte oder betrügerische Domains zu identifizieren, die legitime Adressen nachahmen.

Für eine zielgerichtete Analyse nicht indexierter oder weniger bekannter Domains kann auch die Suchfunktion von <https://urlscan.io> verwendet werden. Beispielsweise erlaubt eine Suche wie `page.domain:*osint*` das Auffinden aller gescannten Seiten, deren Domains das Stichwort `osint` enthalten. Für diese Suche ist jedoch ein Log-in notwendig.

Netzwerkdaten

Seit dem Inkrafttreten der DSGVO und der zunehmenden Nutzung von Whois-Privacy-Anbietern ist ein direkter Abruf von Whois-Daten oftmals nicht möglich. Dennoch können die Daten in den meisten Fällen angefragt werden. Interessant ist die inverse Suche oder Rückwärtssuche von Whois-Daten. Außerdem kann überprüft werden, welche weiteren Domains unter einer IP-Adresse erreichbar sind.

Es gibt einige hilfreiche Online-Dienste für diese Analysen:

- ▶ *Host.io* (<https://host.io>) bietet umfassende Such- und Filtermöglichkeiten zu IP-Adressen, Domains, Subdomains und deren Verbindungen, inklusive Whois- und SSL-Daten.
- ▶ *Digger.tools* (<https://digger.tools>) ermöglicht die Recherche von Domain-, IP- und Hosting-Informationen, inklusive Reverse-DNS und Subdomain-Aufspüren.
- ▶ *DNSDumpster* (<https://dnsdumpster.com>) ist ein kostenloses Tool, das DNS-Records, Hosts und Subdomains einer Domain visualisiert und oft Rückschlüsse auf zusätzliche Infrastruktur erlaubt.

Auch über *Shodan* können Sie Informationen zu einer Domain abrufen. Ersetzen Sie hierzu in der URL <https://beta.shodan.io/domain/<domain>> `<domain>` durch die zu untersuchende Domain. Anschließend erhalten Sie eine Übersicht über DNS-Einträge sowie bekannte Subdomains.

Zertifikate

crt.sh (<https://crt.sh/>) ist eine öffentlich zugängliche Datenbank, die Einträge der *Certificate Transparency* aufbereitet. Die CT-Logs dokumentieren alle von anerkannten Zertifizierungsstellen ausgestellten SSL/TLS-Zertifikate. Die Plattform bietet Einsicht in alle Zertifikate, die für eine bestimmte Domain ausgestellt wurden, einschließlich historischer Daten, abgelaufener Zertifikate und Subdomains.

Neben *crt.sh* bietet auch *Shodan* Zugriff auf SSL-Zertifikate, die bei Netzwerk-Scans gefunden wurden. Auch *Digger.tools* (<https://www.digger.tools>) zeigt Ihnen im Tab CERTS eine Übersicht über die Zertifikate für eine Domain.

CertStream (<https://certstream.calidog.io/>) ist ein weiterer Live-Daten-Feed, der die CT-Logs auswertet. Er erlaubt die unmittelbare Beobachtung neu ausgestellter SSL/TLS-Zertifikate, noch bevor diese in anderen Tools auftauchen.

Technischer Fingerabdruck

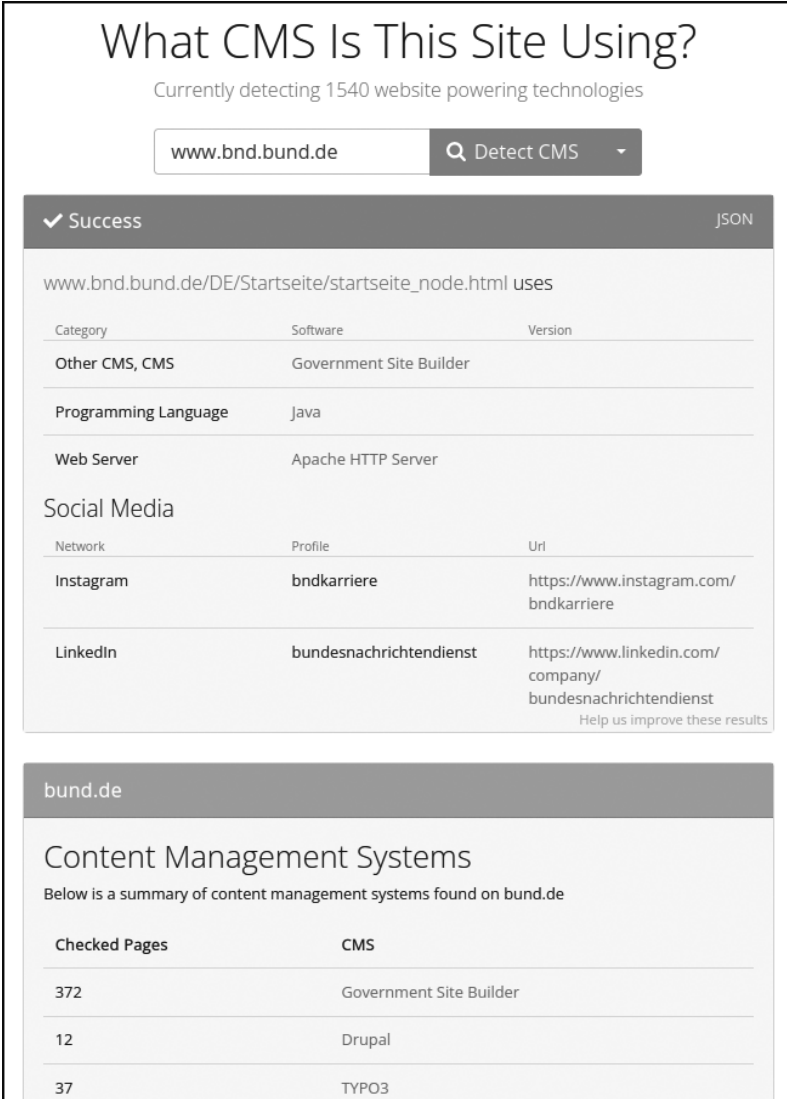
Ein technischer Fingerabdruck bezeichnet in der IT- und Sicherheitsbranche die charakteristische Zusammenstellung von Merkmalen einer Webseite, eines Servers oder eines Endgeräts. Diese Merkmale erlauben es, sie eindeutig zu identifizieren oder zumindest stark zu charakterisieren.

Online-Tools wie jene von Netcraft (<https://sitereport.netcraft.com/>) geben einen Überblick über die eingesetzten Technologien. Sie liefern das Serverbetriebssystem, den Webservertyp, Hosting-Provider und weitere Infrastrukturdetails.

Eine weitere Möglichkeit bietet das Online-Tool *What CMS*, das Sie unter <https://whatcms.org> finden. Bei der Namensfindung waren die Betreiber zwar nicht sehr kreativ, aber so wissen Sie, was Sie von dem Tool erwarten können: Es gibt Auskunft darüber, welches *Content Management System (CMS)* bzw. welche Technologien eine Website verwendet.

Um eine Abfrage zu starten, geben Sie einfach die URL in die Suchmaske ein und klicken auf den Button DETECT CMS. Sie können über das Dropdown-Menü zusätzliche Abfragemöglichkeiten aufrufen, um den Hosting-Provider oder das Design-Template zu erkennen.

Geben wir nun in das Suchfeld beispielsweise »www.bnd.bund.de« ein, erhalten wir einen Augenblick später das Ergebnis.



What CMS Is This Site Using?
Currently detecting 1540 website powering technologies

www.bnd.bund.de

✓ Success JSON

www.bnd.bund.de/DE/Startseite/startseite_node.html uses

Category	Software	Version
Other CMS, CMS	Government Site Builder	
Programming Language	Java	
Web Server	Apache HTTP Server	

Social Media

Network	Profile	Url
Instagram	bndkarriere	https://www.instagram.com/bndkarriere
LinkedIn	bundesnachrichtendienst	https://www.linkedin.com/company/bundesnachrichtendienst

Help us improve these results

bund.de

Content Management Systems

Below is a summary of content management systems found on bund.de

Checked Pages	CMS
372	Government Site Builder
12	Drupal
37	TYPO3

Abbildung 7.105 Der Bundesnachrichtendienst nutzt den Government Site Builder

Wie Sie in Abbildung 7.105 sehen, nutzt der Bundesnachrichtendienst das CMS *Government Site Builder*. Darüber hinaus ist ersichtlich, dass die Programmiersprache Java und ein Apache-Webserver eingesetzt werden. Möglicherweise haben Sie den kleinen Texthinweis »JSON« entdeckt. Leider verbirgt sich dahinter nicht das Ergebnis im JSON-Format, sondern lediglich die Dokumentation, die Ihnen beschreibt, wie Sie die Antwort im JSON-Format erhalten. Dazu benötigen Sie allerdings einen API-Key. Eine nette Zusatzfunktion ist allerdings die Extraktion von Verlinkungen zu sozialen Netzwerken, die Sie im Abschnitt SOCIAL MEDIA sehen können. Darüber hinaus erhalten Sie eine Zusammenfassung gefundener Content-Management-Systeme auf der gesamten Domain *bund.de* sowie zuvor überprüfte oder in anderen Fällen bisher nicht gescannte Seiten.

Bleiben wir einen Moment beim Ergebnis für die BND-Website. Tatsächlich handelt es sich bei den blau eingefärbten Textelementen um Verlinkungen, z. B. zu den Social-Media-Accounts des BND.

Wenn Sie nun auf GOVERNMENT SITE BUILDER klicken, werden Sie auf eine Übersichtsseite zu dem CMS oder der Technologie geleitet. So finden Sie heraus, dass der Government Site Builder von der Bundesrepublik Deutschland u. a. für Ministerien oder andere Teile der Verwaltung eingesetzt wird. *What CMS* kennt 418 Webseiten, die diese Technologie nutzen. Leider erhalten Sie diese Liste nur, wenn Sie einen Account und ein kostenpflichtiges Abonnement haben. Wenn Sie die Übersichtsseite jedoch hinunterscrollen, finden Sie einen Abschnitt mit populären Webseiten, die diese Technologie nutzen.

Mit *NerdyData* (<https://www.nerdydata.com/reports/new>) können Sie nach Webseiten suchen, die eine bestimmte Technologie einsetzen. Alternativ können Sie aber auch zu einer Domain die genutzten Technologien abfragen.

Source Code

Mit der Suchmaschine *PublicWWW* (<https://publicwww.com/>) können Sie insbesondere den Quelltext von Webseiten durchsuchen. In der kostenlosen Version erhalten Sie die Ergebnisse der 3 Millionen bekanntesten Websites. Unter <https://publicwww.com/syntax.html> finden Sie eine Übersicht der Abfragesyntax.

Webseiten stellen über strukturierte Daten zusätzliche Informationen bereit, die von Suchmaschinen besser interpretiert werden können. Das *Schema.org*-Markup, unterstützt von Google, Microsoft, Yahoo und Yandex, stellt ein einheitliches Vokabular zur semantischen Anreicherung von Inhalten bereit. Dies kann einerseits als Microdata direkt in die HTML-Tags eingebracht werden, andererseits per *Resource Description Framework (RDFa)* oder per *JSON-LD* integriert werden.

Mit dem Validator von *Schema.org* können Sie eine Webseite auf strukturierte Daten überprüfen (siehe Abbildung 7.106). Rufen Sie dazu die Webseite unter der URL <https://validator.schema.org/> auf, geben Sie die URL der zu prüfenden Webseite in das Pop-up-Feld ein und klicken Sie auf TESTEN. Nach kurzer Zeit sehen Sie auf der linken Seite den Quelltext und auf der rechten Seite die gefundenen strukturierten Daten in Form von Kartenansichten. Wenn Sie auf eine der Karten klicken, werden die verfügbaren Informationen angezeigt.

The screenshot shows the Schema.org validator interface. The browser address bar displays <https://osintgeek.de/>. The left pane shows the HTML source code, and the right pane displays the detected structured data. The detected data includes:

Erkannt	0 FEHLER	0 WARNUNGEN	3 ELEMENTE
Organization	0 FEHLER	0 WARNUNGEN	1 ELEMENT
LocalBusiness	0 FEHLER	0 WARNUNGEN	1 ELEMENT
WebSite	0 FEHLER	0 WARNUNGEN	1 ELEMENT

Abbildung 7.106 Ergebnis zur Seite »osintgeek.de«

Diese Tools helfen Ihnen, nicht nur die sichtbaren Inhalte für Ihre Recherche zu nutzen, sondern auch den darunterliegenden Quelltext.

Inhalte

Eine Webseite präsentiert Daten über das Internet. Der Umfang einer Webseite kann von einfachen Textinformationen bis hin zu komplexen Webanwendungen variieren. Aus den Daten können Informationen gewonnen werden. Zu den Informationen gehören:

- ▶ Texte
 - Inhalt
 - Namen
 - Adressen
 - Rufnummern
 - Nutzernamen

- Bezahlungen/Kontoverbindung
- Grammatik
- Rechtschreibung
- ausgefallene Formulierungen/Redewendungen
- ▶ Bilddateien
- ▶ Verlinkungen
- ▶ Quellcode
 - Kommentare
 - Unique Identifier, Trackingcodes
- ▶ verwendete Software

Zur Erstellung eines Webseiten-Fingerabdrucks eignen sich Informationen über das Hosting sowie Informationen über die verwendete Software. Heutzutage gibt es Unmengen an Varianten, wie eine Webseite erstellt werden kann. Eine Möglichkeit, um die zugrundeliegende Technik herauszufinden, ist eine Analyse des Quelltextes. Dies erfordert jedoch technisches Wissen.

Eine einfache Methode ist der Onlinedienst *BuiltWith* (<https://builtwith.com/>). Über eine einfache Eingabe der URL erhält man Informationen über die verwendete Software.

Neben Inhalten spielen auch spezielle Dateien eine Rolle:

- ▶ Die `robots.txt` steuert Suchmaschinen-Crawler und zeigt, welche Bereiche einer Webseite vom Indexieren ausgeschlossen sind, was Rückschlüsse auf versteckte oder sensible Bereiche erlaubt.
- ▶ Die `security.txt` ist ein Standard zur Veröffentlichung von Kontaktdaten für die Sicherheitskommunikation, z. B. für Meldungen zu Schwachstellen.

Kennen Sie das *Favicon*? Es handelt sich hierbei um ein kleines, quadratisches Icon, das eine Webseite hinterlegen kann und dann von Webbrowsern, meist im Tab, dargestellt wird. Doch dieses ursprünglich nur 16 × 16 Pixel große Symbol ist nicht zu unterschätzen. Denn ähnlich wie bei einer Bilderrückwärtssuche kann auch das Favicon genutzt werden, um beispielsweise weitere Webseiten zu finden, die ebenfalls ein bestimmtes Icon verwenden.

Um gezielt nach dem Favicon zu suchen, verwendet man einen Hashwert, der anhand des Favicons errechnet wird. Je nachdem, welche Plattform für die Suche genutzt wird, benötigt man *MurmurHash3*, *md5* oder *sha256*. Auf der Website <https://favicon-hash.kmsec.uk> finden Sie den *Favicon Hash Generator*, der Ihnen anhand einer URL oder Datei die Hashwerte liefert. Praktischerweise werden Buttons für die Suche nach dem jeweiligen Hash für *Shodan*, *VirusTotal* und *Censys* gebildet.

Das Alter einer Domain lässt sich mit dem Domain-Age-Checker (<https://tools.verify-emailaddress.io/Apps/Domain-Age-Checker>) in Erfahrung bringen. Bei der Überprüfung des Alters einer Domain ist das Python-Programm *Carbon14* (<https://github.com/Lazza/Carbon14>) hilfreich, da es die Zeitstempel von eingebundenen Bildern ausgibt.

Zur Erkennung von Phishing oder weiteren Sicherheitsrisiken empfehlen sich spezialisierte Dienste wie <https://openphish.com>, die bekannte Phishing-Domains und URL-Listen bereitstellen, sowie das Tool *FOCA* (<https://github.com/ElevenPaths/FOCA>), mit dem Metadaten in Dokumenten und Webseiten analysiert werden können.

Darüber hinaus können Sie selbstverständlich sämtliche Bilder für inverse Bildsuchen verwenden oder Textpassagen über die exakte Suche recherchieren.

Verhalten und Traffic

Malware-Analyseplattformen sind Werkzeuge zur Identifizierung und Untersuchung von Malware, die auf Webseiten oder in Netzwerken entdeckt wird. Über solche Plattformen lässt sich Malware in einer sicheren und isolierten Umgebung untersuchen: Wie verhält sie sich, welche Systemressourcen nutzt sie – und was ist das Schädliche an ihr?

Zu den gängigen Malware-Analyseplattformen gehören *VirusTotal* (<https://www.virustotal.com>), das Dateien und URLs mithilfe verschiedener Antivirenprogramme überprüft, sowie *Joe's Sandbox* (<http://joesandbox.com>) und *Hybrid Analysis* (<https://www.hybrid-analysis.com>), die tiefgreifendere Verhaltensanalysen und Berichte bieten.

Mit den *Traffic-Checker-Tools* von Ahrefs (<https://ahrefs.com/traffic-checker>) und SE Ranking (<https://seranking.com/website-traffic-checker.html>) können Sie den Web-Traffic einer Website analysieren und wichtige Metriken erfassen. So erhalten Sie Einblicke in die monatlichen Besucherzahlen, die Herkunftsländer der Besucher sowie die wichtigsten Keywords, die für Traffic sorgen. Diese Informationen können Ihnen helfen, die Sichtbarkeit und den Einfluss einer Website besser zu verstehen und Traffic-Trends sowie potenziell verdächtige Aktivitäten zu erkennen.

7.11.6 Webarchive

Webinhalte sind einem ständigen Wandel unterworfen und können jederzeit verändert, überarbeitet oder vollständig gelöscht werden. Besonders für OSINT-Analysen, Recherchezwecke und Beweissicherung ist es daher wichtig, auch auf ältere oder inzwischen nicht mehr erreichbare Inhalte zugreifen zu können.

Kapitel 12

Am Ball bleiben

Man lernt nie aus.

Das gilt für fast alles im Leben, trifft aber besonders auf die Arbeit mit Informationen und Daten zu. Ständig gibt es neue Ansätze, Methoden und Tools. Bleiben Sie daher am Ball!

Open Source Intelligence (OSINT) ist von einer immensen Dynamik geprägt. Neue Tools und Technologien erscheinen ständig, Quellen werden zugänglicher oder verschwinden, Plattformen ändern ihre APIs und die rechtlichen Rahmenbedingungen können sich wandeln. Um in diesem Umfeld effektiv zu bleiben, ist eine kontinuierliche Weiterbildung und ein aktives Engagement in der Community unerlässlich. Wer am Ball bleibt, sichert nicht nur die Relevanz der eigenen Fähigkeiten, sondern entdeckt auch neue Ansätze für zukünftige Recherchen.

12.1 Trainingsmöglichkeiten

Theorie ist wichtig, aber OSINT lebt von der praktischen Anwendung. Regelmäßiges Üben und das Lösen von Herausforderungen schärfen Ihre Fähigkeiten, fördern kreative Lösungsansätze und halten Sie auf dem neuesten Stand.

Ein ganz einfacher Tipp ist es, sich regelmäßig selbst zu recherchieren. Zum einen können Sie sofort bewerten, ob die gefundenen Informationen akkurat sind oder nicht. Zum anderen stellen Sie so sicher, digitale Hygiene zu leben, da Sie auf vorhandene Daten schnell reagieren können. Das ist eine hervorragende Übung.

Das Einverständnis vorausgesetzt, können Sie diese Übung auf Personen aus Ihrem näheren Umfeld ausweiten und diesen Ratschläge geben, welche Informationen gegebenenfalls missbraucht werden können und deshalb besser geschützt werden sollten. Eine weitere Möglichkeit ist es, selbst Informationen zu verifizieren, die Sie beispielsweise aus der Berichterstattung oder in Social Media aufschnappen.

12.1.1 Praktische Übungen und Challenges

Um Ihre OSINT-Fähigkeiten gezielt zu trainieren und zu vertiefen, bieten sich verschiedene Plattformen und Herausforderungen an. *Quiztime* beispielsweise veröf-

fentlicht regelmäßig kleine Rechercheaufgaben, die sich oft auf Geolokalisierung, aber auch auf die Bestimmung von Zeit oder Kontext beziehen. Ein großer Mehrwert liegt hier nicht nur im Finden der Lösung, sondern auch in der Möglichkeit, die Lösungswege anderer Experten zu studieren und dadurch vielfältige neue Techniken zu erlernen.

Ergänzend dazu bietet *TryHackMe* interaktive »Rooms«, wie zum Beispiel <https://tryhackme.com/room/ohsint>, die speziell darauf ausgelegt sind, verschiedene OSINT-Fertigkeiten in einer praxisnahen Umgebung zu trainieren. Für spielerisches Training Ihrer Geolokalisierungsfähigkeiten sind *Geoguessr* (<https://www.geoguessr.com>), *Geotastic* (<https://geotastic.net>) oder *TimeGuessr* (<https://timeguessr.com/>) tolle Optionen.

Hier werden Sie an zufällige Orte auf der Welt versetzt und müssen anhand von Umgebungsinformationen den genauen Standort bestimmen. Wer sein technisches Verständnis und seine Recherchefähigkeiten im OSINT-Kontext verbessern möchte, findet bei *Sourcing Games* (<https://sourcing.games>) kleine Aufgaben in verschiedenen Schwierigkeitsgraden.

Darüber hinaus finden Sie auf Webseiten wie der von Sofia Santos (<https://gralhix.com/list-of-osint-exercises/>) eine Auswahl an OSINT-Übungen, oft inklusive Lösungen, um Ihre Fähigkeiten gezielt zu trainieren. Eine weitere Möglichkeit sind die Bellingcat-Herausforderungen auf <https://challenge.bellingcat.com/>.

12.1.2 OSINT 4 Good

Nutzen Sie Ihre OSINT-Fähigkeiten auch für gemeinnützige Projekte oder ehrenamtliches Engagement. In viele Hilfsorganisationen, beispielsweise beim Technischen Hilfswerk (THW) mit seinem *Virtual Operations Support Team (VOST)*, können Sie Ihr Wissen und Ihre Fertigkeiten sinnvoll einsetzen: https://www.thw.de/SharedDocs/Einheiten/DE/006_vost.html

Ein anderes Projekt ist die Initiative *Stop Child Abuse – Trace an Object* (<https://www.europol.europa.eu/stopchildabuse>) von Europol. Hier werden Fragmente aus Missbrauchsdarstellungen von Kindern veröffentlicht, die zur Identifizierung von Orten oder Gegenständen dienen können. Indem Sie hier präzise Hinweise liefern, können Sie aktiv dazu beitragen, Kinder aus solchen Situationen zu befreien und die Ermittlung von Tätern zu unterstützen.

Wichtiger Hinweis

Seien Sie im Bereich der Verbrechensbekämpfung stets äußerst zurückhaltend. Mischen Sie sich keinesfalls in laufende Ermittlungen ein, es sei denn, es handelt sich um eine explizite öffentliche Fahndung oder eine offizielle Initiative wie die von Euro-

pol. Unautorisierte Eigenrecherchen können Ermittlungen behindern oder Sie selbst in Gefahr bringen.

12.2 Austausch

Der aktive Austausch mit anderen Praktizierenden ist wichtig, um im dynamischen OSINT-Feld relevant zu bleiben und das eigene Wissen kontinuierlich zu erweitern. Fachkonferenzen bieten eine hervorragende Plattform hierfür, wie beispielsweise die *German Open Source Intelligence Conference (GOSINTCon)* (<https://gosintcon.de>). Diese deutschsprachige Konferenz, die vor einigen Jahren von Matthias Wilson und mir ins Leben gerufen und organisiert wurde, dient dem persönlichen Austausch, dem Knüpfen von Kontakten und dem direkten Lernen von führenden Experten.

12.3 Blogs

Blogs sind eine hervorragende Anlaufstelle, um fundiertes und tiefergehendes Wissen zu erlangen, neue Tools und Techniken kennenzulernen und die Denkweisen erfahrener OSINT-Experten nachzuvollziehen.

- ▶ Beispielsweise bleibt *Sector035* (<https://sector035.nl>) trotz derzeitiger Pause eine großartige Quelle; besonders bekannt ist die informative Reihe *Week in OSINT*.
- ▶ Steven Harris veröffentlicht auf seinem Blog *Nixintel* (<https://nixintel.info>) detaillierte Beiträge, die teilweise technische Details seiner Recherchen offenbaren und so spannende Einblicke liefern.
- ▶ Auch Nico Dekens, bekannt als *Dutch Osint Guy*, verfasst unter <https://www.dutchosintguy.com/blog> regelmäßig Fachartikel zu aktuellen OSINT-Themen – kritisch, reflektiert und praxisnah.
- ▶ Rae Baker schreibt auf ihrem Blog <https://www.raebaker.net/blog> zu verschiedenen OSINT-Themen mit Fokus auf praktische Anwendungen.
- ▶ Griffin Glynn betreibt den Blog *Hatless1der* (<https://hatless1der.com>), der sich auf spezialisiertes OSINT-Wissen konzentriert, oft mit Fokus auf Infrastruktur-, Netzwerk- und technische Ermittlungen.
- ▶ Sofia Santos betreibt den Blog *Gralhix* (<https://gralhix.com/category/blog-entries/>) und schreibt dort sehr praxisbezogen über Recherchen und OSINT-Themen. Ihre Blogbeiträge geben konkrete Einblicke in moderne OSINT-Methoden, digitale Recherche und Geolokation.

12.4 News

Angesichts der rasanten Entwicklungen im Bereich OSINT ist es eine ständige Herausforderung, den Überblick zu behalten. Statt eigenem Monitoring und regelmäßiger Recherche können Sie die Arbeit auch outsourcen, indem Sie auf relevante Informationsquellen setzen.

RSS-Feeds

Um die Informationsflut effizient zu bewältigen, sind RSS-Feeds und News-Aggregatoren unerlässlich. Sie ermöglichen es Ihnen, Nachrichten von einer Vielzahl von Quellen an einem zentralen Ort zu abonnieren und zu verfolgen, ohne jede Website einzeln besuchen zu müssen. Die meisten Blogs bieten RSS-Feeds an.

Newsletter

- ▶ Der *OSINT Jobs Newsletter* (<https://www.osintnewsletter.osint-jobs.com>) hält Sie nicht nur über Jobangebote, sondern auch relevante Branchen-News auf dem Laufenden.
- ▶ Ganz ähnlich ist es mit dem Newsletter von *Forensic OSINT*, den Sie unter <https://www.forensicosint.com/newsletter> abonnieren können.
- ▶ Für aktuelle Beiträge, Tool-Empfehlungen und persönliche Einblicke können Sie sich auch bei meinem Newsletter auf <https://osintgeek.de> anmelden.

Podcasts und Videos

Ein anderes Format bietet der Podcast *OSINT Studio* (<https://osint.studio>). Hier können Sie lauschen, wie Matthias Wilson und ich über unser Lieblingsthema fachsimpeln und neuste Entwicklungen diskutieren. Das Audioformat ermöglicht es Ihnen, auch unterwegs oder bei anderen Tätigkeiten auf dem Laufenden zu bleiben.

Neben *OSINT Studio* gibt es eine wachsende Zahl an weiteren Audio- und Videoformaten, die Tutorials, Interviews mit Experten oder Fallstudien anbieten.

- ▶ Benjamin Strick (<https://www.youtube.com/@Bendobrown>) ist bekannt für seine detaillierten Analysen und Visualisierungen, insbesondere im Bereich der Geolokalisierung und der Verifikation von Bild- und Videomaterial in Konfliktgebieten. Seine Beiträge bieten tiefe Einblicke in investigative Methoden.
- ▶ Gary Ruddell (<https://www.youtube.com/@theintellab>) und Ritu Gill (<https://www.youtube.com/@ForensicOSINT>) liefern beide spannende Inhalte zu verschiedenen OSINT-Techniken und Tools.
- ▶ Auf dem YouTube-Kanal der *GOSINTCon* (<https://www.youtube.com/@GOSINT-Con>) oder über die Konferenzwebseite finden Sie eine Auswahl von ehemaligen Vorträgen und Präsentationen.

Kapitel 13

Fazit und Ausblick

In diesem Kapitel werden zentrale Erkenntnisse zusammengeführt und die wachsende Bedeutung von Open Source Intelligence in unterschiedlichen Anwendungsfeldern beleuchtet. Zugleich richtet sich der Blick nach vorn auf neue technische Entwicklungen, komplexere Informationsräume sowie die Notwendigkeit, Qualitätsstandards und analytische Kompetenzen kontinuierlich weiterzuentwickeln.

Hoffentlich hat Ihnen dieses Handbuch die vielfältigen Facetten von Open Source Intelligence nähergebracht. Sie wissen nun, dass OSINT weit mehr ist als die Nutzung von Suchmaschinen. OSINT ist eine systematische, methodische und ethische Herangehensweise, um öffentlich zugängliche Informationen zu sammeln, zu analysieren und in verwertbare Erkenntnisse zu überführen.

Der Erfolg einer OSINT-Recherche hängt nicht allein von der Menge der gesammelten Daten oder der Nutzung der neuesten Tools ab. Viel wichtiger ist die präzise Formulierung der Fragestellung, die kritische Bewertung der Quellen, die zielgerichtete Anwendung der Methoden und die ergebnisoffene Interpretation der Fakten. Die Kombination aus analytischem Denkvermögen, dem Verständnis des Intelligence Cycle und der effizienten Nutzung spezialisierter Werkzeuge bildet das Fundament für aussagekräftige und verlässliche Resultate.

OSINT ist in zahlreichen Kontexten unverzichtbar geworden: von der investigativen Recherche und der Nachrichtenbeschaffung über die Unternehmenssicherheit und Due Diligence bis hin zur Unterstützung von Strafverfolgungsbehörden und der Bekämpfung von Desinformation. Es ermöglicht ein tiefgreifendes Verständnis komplexer Sachverhalte, die Identifizierung von Netzwerken und Akteuren sowie die Verifizierung von Informationen in einer zunehmend undurchsichtigen Informationslandschaft.

Ausblick

Auch wenn ich mich wiederhole: Das Thema OSINT ist sehr dynamisch und wird sich auch in den kommenden Jahren rasant weiterentwickeln. Daraus ergeben sich sowohl Herausforderungen als auch Chancen.

Die exponentiell wachsende Menge an online verfügbaren Daten erschwert zunehmend die Trennung des Relevanten von Irrelevantem. Gleichzeitig werden Informationen fragmentierter und oft in geschlossenen Ökosystemen ausgetauscht, z. B. in Messenger-Diensten und privaten Gruppen. Soziale Netzwerke schotten sich vermehrt ab und erschweren den Zugang zu vormals offenen Daten.

Eine der größten Herausforderungen ist die zunehmende Perfektion von Deep Fakes und generativen KI-Inhalten. Dadurch gewinnt die Verifikation von Informationen extrem an Bedeutung. Analysten müssen in der Lage sein, manipulative Inhalte zu erkennen und die Authentizität von Quellen kritisch zu hinterfragen.

Gleichzeitig wird der Bedarf an fachkundigem Personal und spezialisierten OSINT-Dienstleistungen weiter zunehmen. Viele Organisationsbereiche entdecken die Methoden der Informationsgewinnung aus öffentlichen Quellen gerade erst für sich, sei es in der Unternehmenssicherheit, im Risikomanagement oder in der Compliance. Dies befeuert den Bedarf an qualifizierten OSINT-Experten erheblich. Parallel dazu findet eine zunehmende Professionalisierung des Themas statt, die Debatten um ethische Richtlinien und rechtliche Rahmenbedingungen vorantreibt und zu einer stärkeren Standardisierung führen wird.

Trotz dieser Herausforderungen bleibt OSINT ein unverzichtbares und mächtiges Werkzeug. Künstliche Intelligenz und Automatisierung werden die Effizienz von OSINT-Analysen weiter steigern, indem sie bei der Verarbeitung großer Datenmengen, Mustererkennung und der Automatisierung von Routineaufgaben unterstützen.

Erfolg im OSINT-Kontext wird zukünftig noch stärker von einer Kombination aus Neugier, kritischem und kreativem Denken, methodischer Disziplin und der Bereitschaft zur kontinuierlichen Weiterbildung abhängen.

Für Ihren weiteren Weg mit dem Thema Open Source Intelligence wünsche ich Ihnen viel Freude und immer Neugier sowie Durchhaltevermögen, damit Sie Ihre Recherchen möglichst oft erfolgreich abschließen.