# 2. Analisi delle fonti aperte

## Categorie di intelligence

Le categorie di intelligence includono la **HUMan INTelligence** (HUMINT), che si basa principalmente su fonti umane, e comprendono inoltre la **COMmunications INTelligence** (COMINT) e la **SIGnal INTelligence** (SIGINT), entrambe incentrate sull'intercettazione e l'analisi dei segnali comunicativi. Vi rientrano anche la **MeAsurements & Signatures INTelligence** (MASINT), focalizzata sulla raccolta di dati misurabili e caratteristici, la **TECHnical INTelligence** (TECHINT), orientata allo studio di tecnologie e apparecchiature, la **FINancial INTelligence** (FININT), incentrata sull'analisi di transazioni e flussi di capitale, la **GEOspatial INTelligence** (GEOINT), dedicata allo sfruttamento di informazioni a carattere geografico, e la **IMagery INTelligence** (IMINT), talvolta denominata **PHOTo INTelligence** (PHOTINT), che analizza immagini per estrarre informazioni.

Infine, l'OSINT – **Open Source INTelligence** ricorre a dati provenienti da fonti aperte e accessibili al pubblico.

## OSINT

«Definiamo l'OSINT come l'individuazione, la raccolta, lo sfruttamento, la validazione, l'analisi e la condivisione, con clienti interessati ad attività d'intelligence, di dati disponibili al pubblico in formato cartaceo o elettronico, provenienti da fonti non classificate e non segrete (spesso riconducibili alla cosiddetta "letteratura grigia").» (Fleisher, 2008)

Il termine **OSINT** (Open Source INTelligence) si riferisce all'impiego di informazioni liberamente disponibili, reperite da fonti aperte e accessibili al pubblico (senza alcun collegamento con il concetto di software open source). Ciò che caratterizza l'OSINT rispetto ad altre forme di intelligence risiede nel fatto che i dati raccolti non provengono da attività illegali o da operazioni clandestine di intercettazione.

Cosa sia davvero l'OSINT e cosa non lo sia può risultare talvolta poco chiaro. Il testo "NATO Open Source Intelligence Handbook" distingue quattro categorie di informazioni e intelligence tratte da fonti aperte. La prima è l'**Open Source Data** (OSD), costituita dai dati grezzi in formato cartaceo, audiovisivo o orale direttamente provenienti dalla fonte primaria. Segue l'**Open Source Information** (OSI), che consiste in quei dati non classificati sottoposti a un processo editoriale di filtraggio, validazione e presentazione, così da formare un insieme coerente e utilizzabile. L'**Open Source Intelligence** (OSINT) rappresenta invece il prodotto di un'attenta ricerca, selezione, analisi e distribuzione a un pubblico selezionato (come un comandante e il suo staff), concepita per rispondere a uno specifico quesito informativo.

Infine, esiste la versione **Validated OSINT** (OSINT-V), che raggiunge un elevato grado di certezza poiché ricavata dall'integrazione di fonti aperte con intelligence classificata, grazie all'esperienza di professionisti capaci di un'analisi "a tutto campo".

Per quanto tale approccio possa apparire intriso di linguaggio burocratico, esso evidenzia l'importanza e la necessità dell'OSINT in ambito strategico, specialmente nella pianificazione militare e nell'intelligence di alto livello. Tuttavia, l'OSINT che utilizziamo in contesti più operativi o applicazioni quotidiane risulta più pratico, finalizzato a scopi tecnici o tattici e spesso impiegato per valutazioni di sicurezza.

# La necessità di informazioni

La ricerca di informazioni utili al proprio scopo ha sempre rivestito un'enorme importanza nella storia. Già nel VI secolo a.C., Sun Tzu consigliava di "conoscere il proprio nemico", mentre Vegezio, con il celebre "Si vis pacem, para bellum", suggeriva che la pace si ottiene preparandosi alla guerra. Senza andare troppo indietro nel tempo, basta ricordare il periodo della guerra fredda, in cui le operazioni di spionaggio e controspionaggio furono centrali nella definizione degli equilibri geopolitici. Qualunque attacco, per avere successo, necessita infatti di un'adeguata preparazione e di solide informazioni su cui basare la propria strategia.

Con l'evoluzione dei mezzi di comunicazione e l'avvento di nuove tecnologie, il volume di informazioni prodotte è aumentato in modo esponenziale: giornali, libri, radio, televisione, fino ad arrivare all'enorme mole di dati resa disponibile attraverso Internet. L'"esplosione" dei servizi offerti online ha portato milioni di persone, aziende ed enti a mettere in rete, spesso volontariamente, una quantità considerevole di dati che li riguardano, talvolta includendo informazioni che sarebbe stato più prudente non divulgare. Queste informazioni sono accessibili a tutti, generando una mole di dati "open source" che chiunque, in teoria, può analizzare. Più informazioni disponibili, dunque, significano più open source intelligence potenzialmente ricavabile, ma anche un numero maggiore di fonti da esaminare e validare.

È proprio in questa massa sconfinata di dati che opera l'esperto di OSINT. Attraverso la ricerca, l'esame e la correlazione di informazioni pubblicamente disponibili è possibile ottenere un quadro su un'organizzazione, sui progetti in corso, sui processi aziendali e perfino sui singoli individui. Tali informazioni possono risultare utili a competitor o a soggetti con intenti criminali, ma non vanno considerate esclusivamente in chiave negativa. L'OSINT, infatti, può essere sfruttata anche per supportare decisioni strategiche, valutare l'efficacia di campagne di marketing o verificare il "sentiment" e la reputazione online di un brand. Inoltre, un impiego consapevole dell'OSINT può migliorare la sicurezza di un'organizzazione, consentendole di individuare e mitigare potenziali minacce prima che queste si concretizzino.

# Chi utilizza OSINT?

L'OSINT viene utilizzata da un'ampia varietà di soggetti, incluse aziende interessate all'analisi del mercato e alla tutela dei propri interessi, recruiter che valutano il profilo dei

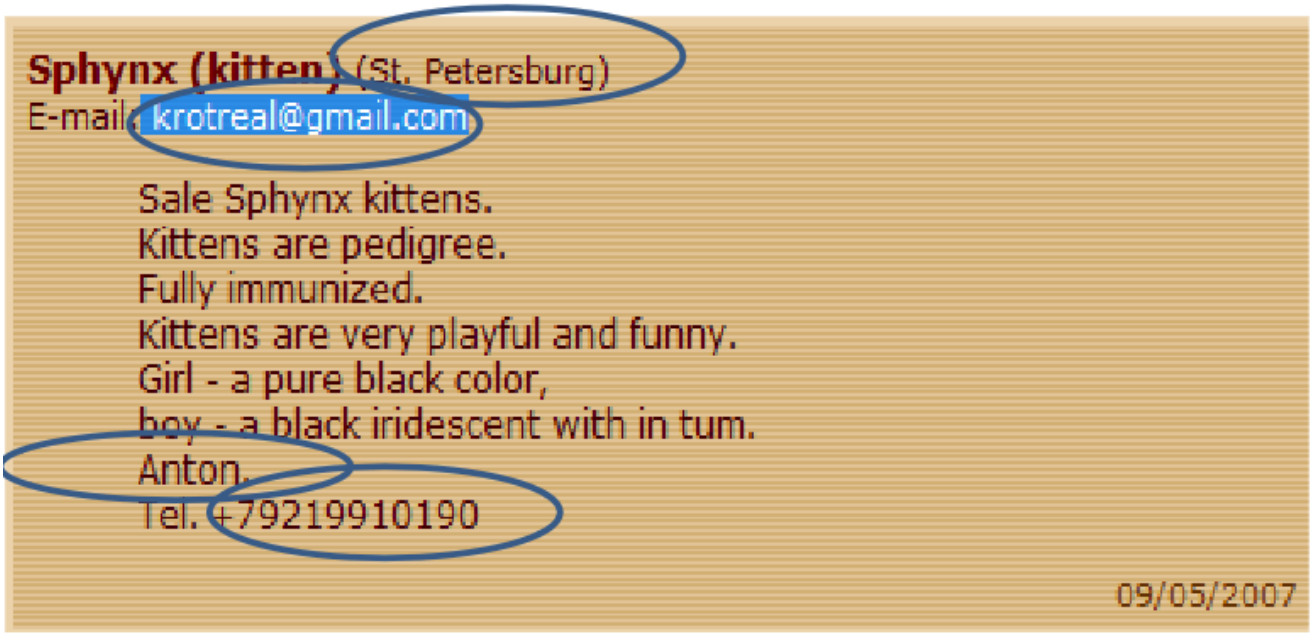
candidati, governi e politici impegnati in attività di intelligence e controspionaggio, forze di polizia, giornalisti d'inchiesta, ma anche investigatori privati, stalker, criminalità organizzata, competitor sleali, semplici buontemponi, troll e criminali informatici. Non sono poi rari gli esempi di "investigazioni" spontanee condotte da analisti indipendenti. Ne è un esempio l'attività dei blogger di Arkenstone, i quali tentano di ricostruire la gerarchia di comando e l'ordine di battaglia dell'esercito iraniano servendosi di risorse a disposizione di tutti. Le loro ricerche si basano, tra l'altro, sull'uso di Google Earth per individuare nuove costruzioni o fortificazioni, sui media iraniani tradizionali come giornali e canali televisivi, sulle parate militari e sugli eventi pubblici, senza dimenticare la cosiddetta "grey literature", ovvero documentazione non classificata, ma non del tutto ufficiale. Con una combinazione di fonti aperte e creatività analitica, questa forma di indagine consente di rivelare dettagli spesso sottovalutati o trascurati.

## Risultati dell'OSINT

L'OSINT può fornire risultati molto diversi in base all'argomento di ricerca, alla competenza di chi la conduce e all'attendibilità delle fonti consultate. Persino l'assenza di un determinato tipo di informazione può costituire un dato significativo. In linea generale, con tempo e risorse adeguate, è possibile ottenere risultati soddisfacenti. Tuttavia, la ricerca a fonti aperte non è esente da problemi. Barriere linguistiche e culturali, fiducia eccessiva negli strumenti automatizzati, disinformazione, informazioni false o manipolate e limitazioni nell'accesso legale a certi dati sono tutti fattori che possono ostacolare il processo e influenzare l'affidabilità delle conclusioni.

L'OSINT offre innumerevoli possibilità di impiego. Nel campo delle risorse umane può essere utilizzata per individuare dipendenti potenzialmente scontenti o per verificare la veridicità dei curriculum di nuovi candidati; su un piano strategico, invece, consente di reperire informazioni personali, monitorare i concorrenti, analizzare trend economici, supportare operazioni di antiriciclaggio e valutare l'impatto di iniziative di marketing. L'impiego di queste tecniche è possibile anche nell'ambito dell'intelligence non classificata di tipo militare, nonché nel controllo di gruppi d'interesse di vario genere.

Il caso Koobface rappresenta un esempio concreto dell'efficacia dell'OSINT. Un singolo errore commesso dal responsabile di una botnet ha permesso a un ricercatore tenace e paziente di ricostruire l'identità del "botnet master", rintracciandone il numero di telefono, il nome e l'indirizzo. Partendo dall'analisi dell'infrastruttura di Koobface e individuando i domini registrati sul medesimo indirizzo IP, il ricercatore ha scoperto un dominio associato a un indirizzo email inconsueto — krotreal@gmail.com — da cui è risalito alle informazioni personali del cybercriminale. Il dettaglio curioso è che, tra i vari dati disponibili, è emerso un annuncio di vendita di gattini Sphynx, a conferma del fatto che persino i criminali lasciano tracce involontarie in rete.




Da questa vicenda si ricava un insegnamento importante: la pigrizia è un grave difetto nel campo della sicurezza, poiché la mancanza di rigore nella gestione dei dati può diventare un punto debole. La sicurezza non è retroattiva e un singolo errore — un file fuori posto, un pacchetto di dati in eccesso, un'informazione non opportunamente ripulita — può esporre a rischi considerevoli anche gli attori più abili e preparati. L'OSINT, dunque, non è soltanto un insieme di tecniche per raccogliere informazioni, ma un monito sulla vulnerabilità intrinseca della presenza online e sulla necessità di una costante attenzione alla protezione dei propri dati.

## Modalità di fare OSINT

Esistono due principali modalità operative per condurre attività di OSINT.

La prima, di tipo **manuale**, implica che la ricerca venga effettuata direttamente dall'analista, il quale prende decisioni sul momento e valuta la qualità delle fonti in tempo reale. Se da un lato questo approccio permette una validazione accurata dei dati, dall'altro comporta un impegno notevole in termini di tempo ed energie, con il rischio di "perdere" informazioni rilevanti e una difficoltà intrinseca nel rendere il processo scalabile.

La seconda modalità, di tipo **automatico**, prevede l'utilizzo di strumenti parametrici e tecnologie avanzate per raccogliere, filtrare e organizzare grandi volumi di dati. Questi sistemi, integrabili con altre soluzioni informatiche, consentono un'elevata scalabilità, ma richiedono ingenti investimenti in termini di hardware e software, oltre ad aggiornamenti continui per stare al passo con l'evoluzione tecnologica. Non va inoltre dimenticato che un'IA non ancora sofisticata come un analista umano può generare falsi positivi, rendendo necessaria una fase di revisione manuale a posteriori.

La soluzione ideale è un approccio **ibrido**, che combina la capacità analitica e critica dell'operatore con la rapidità e la potenza di calcolo dei sistemi automatizzati. In questo modo, l'analista può sfruttare l'efficienza dei metodi automatici per individuare pattern e

collegamenti altrimenti difficili da cogliere, intervenendo poi personalmente nella fase di pulizia, interpretazione e validazione finale dei dati. Questo connubio garantisce un maggiore equilibrio tra efficacia, qualità e scalabilità dell'intero processo di OSINT.

## The art of OSINT

L'arte dell'OSINT risiede nel sottile equilibrio tra l'uso di strumenti tecnologici e l'impiego di capacità umane come intuito, istinto ed esperienza. Per quanto i tool e le API possano automatizzare una vasta gamma di compiti ripetitivi ed estrarre contenuti in modo rapido ed efficiente, riuscire a comprendere appieno il contesto rimane una sfida di ben altro spessore. Il software può organizzare e filtrare dati, ma restituire un quadro coerente e ricco di sfumature richiede l'intervento di un analista in grado di cogliere legami, interpretare segnali deboli e sviluppare ipotesi fondate sulla conoscenza dell'argomento.

L'esperienza maturata nel campo e la familiarità con i vari strumenti sono ciò che distinguono i buoni risultati dai prodotti scadenti. Un semplice username, ad esempio, può rappresentare il punto di partenza per risalire a ulteriori profili riconducibili allo stesso individuo o a persone a lui vicine, rivelando dettagli capaci di condurre all'identità reale, all'indirizzo fisico o addirittura alla geolocalizzazione del bersaglio. L'intero processo di scoperta si basa sulla capacità di tracciare connessioni significative tra frammenti di informazione apparentemente distanti, trasformando dati grezzi in conoscenza utile.

## Link analysis e mind mapper

L'analisi dei collegamenti (link analysis) è una tecnica di analisi dei dati tipica della teoria delle reti, utilizzata per valutare le relazioni tra nodi di diversa natura, quali organizzazioni, individui o transazioni. Questa disciplina punta a individuare e comprendere i legami invisibili tra varie entità, fornendo una visione d'insieme più chiara e coerente. Un approccio analogo, ma orientato alla struttura e all'organizzazione del pensiero, è quello delle mappe mentali, teorizzate dal cognitivista inglese Tony Buzan. Le mind map aiutano a visualizzare in forma grafica idee, appunti e concetti, creando una rappresentazione immediata e intuitiva di informazioni spesso complesse.

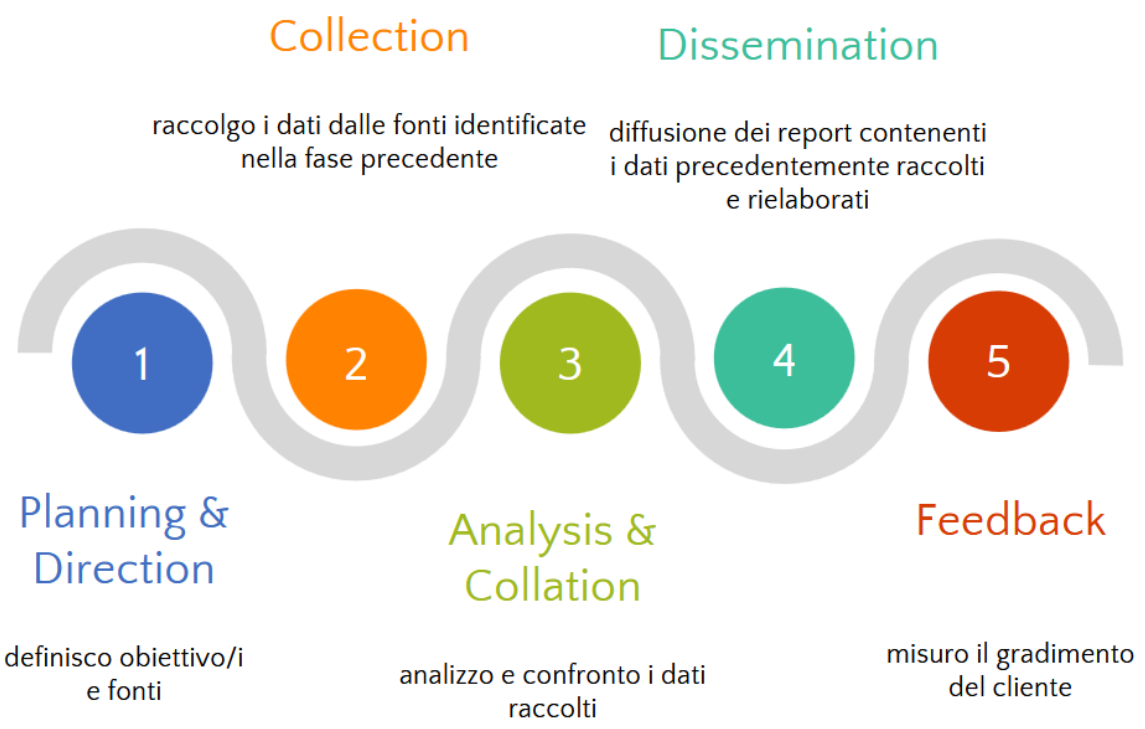
Nell'ambito dell'OSINT, l'uso di software per il "mind mapping" può costituire un valido ausilio nelle attività investigative, facilitando la correlazione dei dati raccolti e la scoperta di pattern altrimenti difficili da riconoscere. Tra gli strumenti disponibili spiccano soluzioni multipiattaforma come VYM (View Your Mind), accessibile all'indirizzo http://sourceforge.net/projects/vym/, Xmind (http://www.xmind.net/) e Freemind (http://freemind.sourceforge.net/). Questi programmi permettono di organizzare visivamente le informazioni, supportando l'analista nella ricerca, nella correlazione e nell'interpretazione di elementi critici per l'attività di OSINT.

## Profiling e scoping

L’attività di profiling e scoping rappresenta un passo cruciale nella conduzione di un’indagine OSINT. Occorre innanzitutto definire con chiarezza il target su cui concentrarsi, stabilire gli obiettivi operativi e fissare regole di ingaggio precise. È importante ricordare che la finalità principale dell’OSINT non è produrre rapporti voluminosi o generici, bensì informazioni puntuali e sfruttabili, in grado di supportare decisioni o orientare strategie.

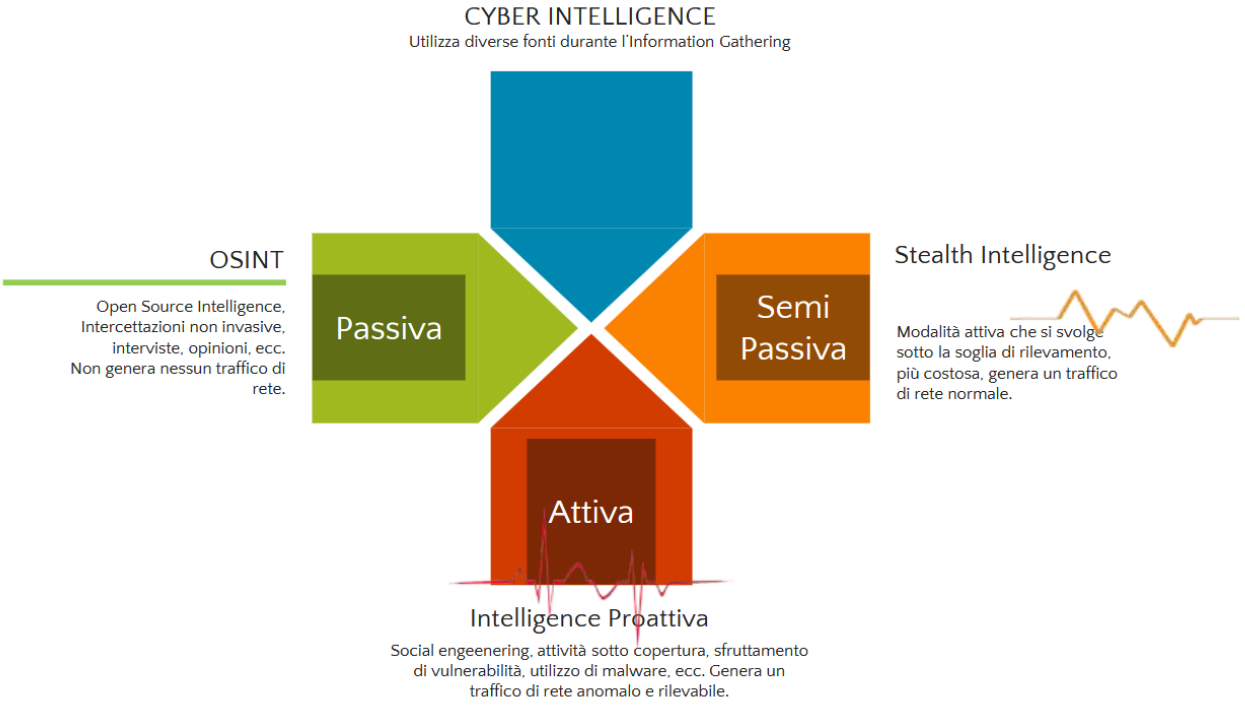
## Pianificazione delle fasi

La pianificazione dell’investigazione parte dalla fase di “Planning & Direction”, in cui si identificano obiettivi e fonti da esaminare. Si procede poi alla “Collection”, la raccolta metodica dei dati secondo quanto definito in precedenza, per passare all’“Analysis & Collation”, che prevede il confronto critico e l’integrazione dei dati raccolti, in modo da estrarne informazioni coerenti e significative. Seguono le fasi di “Dissemination”, in cui i risultati vengono presentati ai destinatari in forma di report utilizzabile, e infine il “Feedback”, fase in cui si valuta il livello di soddisfazione del cliente o del committente e si individuano possibili miglioramenti del ciclo analitico.




## Che tipo di OSINT effettuare?

La scelta del tipo di OSINT da effettuare dipende dal contesto, dagli obiettivi e dalle risorse disponibili. In un quadro più ampio, possiamo distinguere approcci di carattere passivo, semi-passivo e attivo, con alcune forme di “stealth intelligence” che si collocano in un’area meno evidente e più costosa da attuare.




Le attività di OSINT passiva si limitano all'acquisizione di informazioni disponibili pubblicamente senza interagire in modo rilevante con il target o l'ambiente bersaglio. Questo tipo di operazione non genera traffico anomalo e non lascia tracce evidenti, poiché ci si limita all'analisi di fonti aperte come siti web, social media, documentazione pubblica e opinioni reperibili in rete.

Le modalità semi-passive possono includere un maggior grado di interazione, come l'utilizzo di tecniche per individuare servizi o dati aggiuntivi senza tuttavia superare determinate soglie di rilevamento o comportarsi in modo chiaramente sospetto. Si tratta di un approccio più incisivo rispetto a quello passivo, ma meno invasivo o rischioso dell'OSINT attiva.

L'OSINT attiva, invece, comporta un coinvolgimento più diretto, spesso riconducibile a quella che si potrebbe definire "intelligence proattiva". Qui rientrano attività sotto copertura, tentativi di social engineering, l'individuazione e lo sfruttamento di vulnerabilità e l'impiego di malware. Questa modalità può generare traffico di rete anomalo e lasciare potenziali indizi del proprio operato, rendendo necessarie competenze e cautele elevate.

Infine, la "stealth intelligence" si colloca a un livello intermedio tra la modalità attiva e quella semi-passiva: è una forma di raccolta informativa attiva, ma condotta con estrema attenzione per non superare le soglie di allarme. Implica costi maggiori e una progettazione scrupolosa, poiché punta a rimanere sotto il radar generando traffico di rete che appare del tutto normale.

In definitiva, la scelta tra OSINT passiva, semi-passiva, attiva o stealth dovrebbe basarsi su un'attenta valutazione del rischio, degli obiettivi, del livello di sensibilità del target e delle risorse a disposizione. L'analista deciderà quale combinazione di tecniche e approcci risulti più appropriata per soddisfare le esigenze strategiche o operative della situazione in esame.

# Le fonti OSINT

La classificazione delle fonti informative utilizzabili nell'ambito dell'OSINT comprende diverse tipologie. Si parte dalle informazioni generali provenienti dal web o dai media tradizionali, e dalle informazioni a pagamento, spesso contenute in database commerciali o siti che offrono dati strutturati e aggiornati a fronte di un corrispettivo. A queste si aggiungono i contributi degli esperti, come tecnici e specialisti, che, attraverso interviste o opinioni qualificate, possono fornire un valore aggiunto all'analisi. Un'importante categoria è poi rappresentata dai documenti "gray" (come brevetti, report interni, atti di convegni, pubblicazioni non ufficialmente strutturate), spesso ricchi di dettagli non immediatamente noti al grande pubblico.

In questo contesto, si definiscono inoltre gli O.D.S. (Open Source Data), ovvero dati grezzi e generici provenienti da fonti non necessariamente attendibili, disponibili pubblicamente su canali di libero accesso, come registrazioni, immagini satellitari e documentazione varia; e gli O.S.I.F. (Open Source Information), ossia informazioni pubbliche che hanno già subito un processo di filtraggio e convalida, come quelle fornite dai giornali, dai libri o da fonti istituzionali riconosciute. L'OSINT vera e propria nasce dalla fusione di ODS e OSIF: è l'insieme di informazioni non classificate, ma ricercate, filtrate e selezionate per rispondere a domande specifiche e supportare decisioni strategiche o operative.

Per trattare adeguatamente queste fonti, occorre padroneggiare diversi strumenti e tecniche. Ci si avvale di strumenti di hacking "etico" o di investigative tool specifici per individuare identità digitali, si sfrutta un uso avanzato dei motori di ricerca (eventualmente utilizzando risorse come il Google Hacking Database) e si consultano portali di investigazioni online in grado di fornire dati istituzionali su persone fisiche o giuridiche, sugli asset societari, sulle proprietà immobiliari e così via.

Le possibili fonti a cui attingere sono innumerevoli: motori di ricerca e social network, chat (come Skype, IRC o piattaforme private), blog, mailing list, forum, siti di vendita, scambio e annunci, piattaforme per la condivisione di immagini e video, siti di incontri, quotidiani, banche dati pubbliche, registri amministrativi, camere di commercio, archivi pubblici, organizzazioni governative o non governative e siti istituzionali. Anche la cosiddetta "grey literature", il Deep Web, i servizi specializzati nella ricerca e vendita di informazioni, nonché i dati tecnici reperibili in rete costituiscono un bacino di fonti a cui attingere. L'abilità dell'analista OSINT sta proprio nel sapere individuare, valutare e integrare questi diversi flussi di informazione, trasformandoli in conoscenza utile e mirata.

# Metodologie

I metodi per condurre un'investigazione OSINT comprendono diverse tecniche, tra cui la ricerca per parole chiave, l'analisi delle immagini, la correlazione tra le informazioni raccolte, lo studio dell'ambiente di riferimento, l'esame dei contatti del target e l'analisi di dati tecnici riguardanti reti e infrastrutture Internet. Per avviare la ricerca, è utile partire dalle informazioni già disponibili, valutarne i contesti di indagine (ad esempio l'ambito lavorativo o

i rapporti personali) e stabilire una priorità tra le possibili linee d'azione. Da qui nasce la necessità di identificare parole chiave mirate e pertinenti, con la consapevolezza che queste, così come gli argomenti di interesse, possono mutare nel corso del lavoro a seguito di nuovi spunti o risultati.

La flessibilità e la capacità di correlare le diverse risposte ottenute consentono infatti di individuare nuove direzioni di ricerca. Tutto dipende dal soggetto dell'indagine, dalla domanda cui occorre rispondere e dalla qualità dei dati iniziali. Creatività, immaginazione e abilità logiche si combinano con solide conoscenze tecniche e un set di strumenti adeguati, aiutando l'analista a estrarre valore dai dati e orientare il proprio lavoro in modo efficace e mirato.

## Le basi: motori di ricerca

I motori di ricerca rappresentano uno strumento fondamentale, ma spesso se ne sovrastima l'accuratezza e la completezza. Oltre a quelli generici, come Google o Bing, ne esistono di specifici, specializzati su determinati ambiti, dalle ricerche su social network all'individuazione di determinati username, fino ai cataloghi digitali delle biblioteche (ad esempio, il Library of Congress Online Catalog) o ai motori orientati alla ricerca di persone, come Pipl, e persino ai motori di ricerca interni dei singoli siti.

Un errore comune consiste nel dare per scontata l'infallibilità dei motori di ricerca, senza considerare come questi siano in realtà complessi sistemi composti da tre elementi: uno spider o crawler che esplora la rete, un database in cui si indicizzano i contenuti rilevati e un motore di backend che interpreta le richieste, assegna un "rank" alle risorse in base ad algoritmi dinamici e restituisce i risultati. È altrettanto sbagliato assumere che un motore di ricerca valga l'altro. Uno studio condotto su oltre 12.500 query diverse, testate su Yahoo, Google, MSN e Ask Jeeves, ha dimostrato che solo l'1,1% dei risultati appare su tutti e quattro i motori, mentre circa l'85% dei risultati principali è unico di un singolo motore.

Cosa significa tutto questo? Significa che i risultati possono variare notevolmente a seconda del motore di ricerca utilizzato. Di conseguenza, è indispensabile acquisire la capacità di adoperare diversi strumenti, attingere a motori specializzati e sfruttare appieno le funzioni peculiari di ciascuno. Nei prossimi approfondimenti vedremo come utilizzare le caratteristiche distintive di alcuni motori di ricerca per ottenere il massimo dai dati disponibili online.

Google, Yahoo e Bing sono principalmente orientati al mercato statunitense, mentre Baidu è rivolto soprattutto agli utenti cinesi. Un analista OSINT deve saper sfruttare le specificità di ogni motore di ricerca, tenendo presente che ciascuno rispecchia le dinamiche, la lingua e le priorità del Paese o della regione a cui è destinato. È importante ricordare che gran parte degli strumenti di ricerca non statunitensi raccoglie e memorizza dati prevalentemente su scala locale, pertanto si possono reperire informazioni su Yandex che non risultano disponibili su Google.com o persino su Google.ru. L'aspetto linguistico è centrale: i motori internazionali devono consentire la ricerca nella lingua madre, e l'utilizzo di query formulate

con alfabeti non latini può condurre a risultati più puntuali e pertinenti. Saper padroneggiare queste variabili è essenziale per individuare la giusta chiave di accesso a fonti informative spesso ignorate o sottovalutate.

## Social Network

I profili social rappresentano una fonte straordinaria di dati utili all'analisi OSINT. Lo studio attento dei contatti può offrire nuovi spunti d'indagine, consentendo di definire mappe relazionali e di risalire a connessioni non immediatamente evidenti. In passato, uno strumento particolarmente efficace era la funzionalità di Graph Search offerta da Facebook, che permetteva di individuare pattern e relazioni a partire dai profili e dai contenuti condivisi. Tuttavia, dopo il caso Cambridge Analytica, la piattaforma ha modificato radicalmente le proprie politiche di accesso ai dati, limitando la possibilità di interrogare le informazioni attraverso ricerche complesse e mirate.

Tra i social network più diffusi, spiccano i cosiddetti "The Big Ones": Facebook, Twitter e Google+, ormai considerati standard di riferimento per quantità di dati disponibili. Ma anche social più datati, come Myspace, le piattaforme orientate all'immagine e alla notorietà ("Media/Vanity") quali Instagram, Flickr, Vine, Foursquare e YouTube, nonché i social network internazionali che dominano in specifiche aree geografiche, come Weibo in Cina, VKontakte in Russia, Tuenti e Qzone in altre aree del mondo. Non vanno dimenticate, infine, le piattaforme professionali come LinkedIn, che forniscono informazioni di carattere lavorativo e relazionale, potenzialmente molto utili per ricostruire contesti aziendali o settoriali.

In generale, la chiave di una buona indagine OSINT sui social network risiede nella capacità di adeguarsi all'evoluzione continua delle piattaforme, alle loro politiche di privacy, all'imprevedibilità dei dati disponibili e alla necessità di combinare più fonti per individuare legami, pattern e piste di ricerca. L'utilizzo strategico di questi strumenti può fornire uno sguardo ricchissimo sulla sfera personale, professionale e culturale di individui e gruppi, offrendo all'analista elementi preziosi per il raggiungimento degli obiettivi informativi.

## Comunità virtuali

Le comunità virtuali rappresentano tutto ciò che, pur non rientrando nella categoria dei "social network" moderni, in passato costituiva il cuore pulsante di Internet come luogo di scambio, confronto e comunicazione tra gli utenti. Tra queste realtà si annoverano i forum, le mailing list e i blog, piattaforme che nel tempo hanno permesso di creare legami attorno a specifici temi o interessi comuni. Ai margini dei social network si collocano poi le chat online, come quelle basate su IRC, e le comunità legate ai videogiochi, diffuse su servizi quali PlayStation Network, Xbox Live o Steam. Infine, è impossibile trascurare i mondi virtuali, spazi digitali immersivi in cui gli utenti danno vita a interazioni complesse e collaborative, testimoniando l'evoluzione costante delle forme di aggregazione online.

## Selected Source: People

Le persone possono costituire una fonte informativa preziosa, in particolare quando il target dell'investigazione OSINT è un individuo specifico. Diverse piattaforme offrono strumenti utili per cercare informazioni su singole persone, come i motori di ricerca specializzati (ad esempio Spokeo, PeekYou, Lullar e Pipl) o i siti di incontri (Badoo, Twoo, AdultFriendFinder, Nirvam, Datingwebsites.it), in grado di mettere in luce dati altrimenti difficili da reperire.

## Selected Source: Paste Site

Un'altra tipologia di risorsa è rappresentata dai "Paste Site", strumenti semplici, popolari e in buona misura anonimi, dove gli utenti condividono contenuti di vario tipo. A scopi legittimi ("white"), questi siti vengono impiegati per pubblicare configurazioni, log di crash, frammenti di codice o conversazioni IRC. D'altro canto, in ambito illegale ("black"), i "Paste Site" ospitano spesso file sottratti, database rubati, credenziali trafugate o annunci di vendita di carte di credito compromesse. Aggregatori come netbootcamp.org/pastesearch.html o il celebre Pastebin.com consentono di individuare e analizzare questo genere di contenuti, potenzialmente preziosi per un'indagine.

## Selected Source: Wikipedia

Wikipedia, con oltre un milione e mezzo di voci in italiano, quasi sei milioni in inglese e contenuti disponibili in più di 290 lingue, rappresenta una fonte di informazioni imponente, contribuendo a plasmare la cultura online. Ogni modifica, inserimento o rimozione di contenuti su questa piattaforma è associata a un nome utente o a un indirizzo IP, il che può talvolta permettere di risalire all'autore degli interventi. Una persona di interesse potrebbe essere un collaboratore abituale di Wikipedia, lasciando tracce nei suoi contributi, soprattutto se si occupa di argomenti di nicchia. Tuttavia, occorre tenere presente che Wikipedia, in quanto progetto comunitario, può essere soggetta a manipolazioni, disinformazione o vere e proprie azioni di propaganda. Per esempio, nel 2013 un indirizzo IP riconducibile al Senato degli Stati Uniti modificò la voce su Edward Snowden, definendolo non più "dissidente" ma "traditore".

Strumenti come Wikiscanner (ormai non più disponibile) o servizi analoghi (come wikiwatchdog.com) permettevano o permettono di monitorare le modifiche effettuate su Wikipedia in base a specifici criteri, ad esempio avvisando quando un IP riconducibile a un'istituzione particolare interviene su una pagina sensibile. Queste soluzioni consentono di scoprire, oltre al contenuto informativo, eventuali attività sospette, atti di propaganda o manipolazioni deliberate, trasformando Wikipedia e i suoi dintorni in un terreno fertile per l'attività di OSINT.

I2P, acronimo di Invisible Internet Project, è una rete di anonimizzazione che opera come un'infrastruttura crittografata sovrapposta alla rete Internet standard. Si presenta come una "rete nella rete" che mira a proteggere le comunicazioni dal monitoraggio sistematico da parte di terzi, come ad esempio gli ISP. Attraverso I2P, gli utenti possono navigare e comunicare in modo anonimo, minimizzando il rischio che i loro scambi di informazioni

vengano tracciati o censurati. Ulteriori dettagli sono disponibili sul sito ufficiale: https://geti2p.net/it/.

## Altri strumenti

Freenet, invece, è una rete decentralizzata concepita fin dalla sua origine per resistere alla censura. Sfruttando le risorse messe a disposizione dagli utenti, come larghezza di banda e spazio su disco, Freenet permette di pubblicare e accedere a qualsiasi tipo di informazione senza timore di controlli esterni. La priorità di questa rete è l'anonimato e la sicurezza dei suoi utenti, piuttosto che la velocità di trasmissione dei dati. Freenet è distribuita come software libero sotto licenza GNU General Public License e, essendo scritto in Java, può funzionare su tutti i sistemi operativi che supportano la Java Virtual Machine. Ulteriori informazioni su questa tecnologia sono disponibili all'indirizzo https://freenetproject.org/.

Nel variegato panorama delle reti anonime e dei servizi non indicizzati dai motori di ricerca tradizionali, esistono numerosi strumenti per cercare informazioni all'interno del Dark Web. Tra questi figurano motori dedicati quali Torch, DuckDuckGo (nella sua versione .onion), Onion URL Repository, Uncensored Hidden Wiki, The WWW Virtual Library, notEvil, ParaZite, TorLinks, StartPage, AHMIA, Haystak, Visitor, DarkWeb, Onionland, Deeplink, PirateBay, Abiko, FreshOnions, Candle, Grams, Multivac e Atlayo. L'impiego di questi servizi richiede un approccio consapevole e attento, poiché le reti come Tor ospitano contenuti di vario genere e provenienza, e l'anonimato non garantisce automaticamente la sicurezza o l'affidabilità delle fonti.

In generale, non ci sono soluzioni miracolose in ambito OSINT, ma esistono ottimi strumenti pensati per automatizzare operazioni ripetitive o di routine. È essenziale, però, considerare attentamente ciascun risultato alla luce del contesto in cui lo si colloca: la qualità dell'analisi dipende dalla capacità dell'operatore di filtrare, interpretare e comprendere le informazioni, non solo dalla potenza degli strumenti utilizzati.

# Motori di ricerca: Google

L'utilizzo di Google come motore di ricerca per l'OSINT richiede una comprensione avanzata degli strumenti e delle tecniche a disposizione. Sebbene Google sia una fonte preziosa, non bisogna dimenticare che i risultati variano a seconda della versione locale del motore, della lingua selezionata e della posizione geografica dell'utente. Le differenze possono essere significative, ad esempio, tra gli esiti di una ricerca condotta da un IP cinese, norvegese o statunitense.

## Google Operators

Per migliorare l'efficacia della ricerca, Google fornisce operatori logici e filtri speciali.

Gli operatori di base di Google consentono di effettuare ricerche più precise e mirate. Utilizzando AND in maiuscolo, ad esempio, si richiede che entrambi i termini siano presenti nei risultati (ad esempio, "green AND blue"). Con OR, invece, si impone che almeno uno dei

termini sia presente (come “green OR blue”). Impiegando il segno meno (−) davanti a una parola, è possibile escludere i risultati contenenti quel termine, mentre con l’asterisco (*) si utilizza una wildcard, permettendo così di ricercare eventuali variazioni della parola. Le virgolette (“”) indicano a Google di restituire soltanto i risultati in cui la frase appare esattamente così come è stata digitata. Sfruttando opportunamente questi operatori, l’analista può restringere l’insieme dei risultati a quelli più pertinenti alla propria ricerca.

## Google Dorks

Le cosiddette “Google Dorks” sono query avanzate che sfruttano parole chiave e operatori per applicare filtri particolarmente raffinati. Questi operatori di ricerca avanzata consentono di affinare notevolmente i risultati ottenuti con Google.

In particolare, “**intext**” permette di individuare pagine in cui una determinata parola chiave compare nel testo, mentre “allintext” **ricerca** tutte le parole fornite tra i contenuti della pagina. Con “**inurl**” si cercano URL che contengano almeno una delle parole chiave, mentre “**allinurl**” richiede la presenza di tutte le parole specificate nell’indirizzo. Gli operatori “**intitle**” e “**allintitle**” funzionano in modo analogo, ma limitano la ricerca alle parole presenti nel titolo delle pagine.

L’operatore “**site**” consente di restringere i risultati a un determinato dominio, facilitando la ricerca di informazioni all’interno di un singolo sito web. “**filetype**” isola i documenti in base alla loro estensione, mentre “**link**” individua i collegamenti esterni che puntano a una pagina. “**numrange**” è utile per individuare numeri specifici, mentre “**daterange**” permette di limitare i risultati a un determinato intervallo temporale. Con “**related**” è possibile ottenere siti simili a quello indicato, mentre “**cache**” mostra una versione memorizzata da Google di una pagina. L’operatore “**info**” fornisce informazioni sul sito, e “**location**” filtra i risultati in base al Paese di origine. Utilizzando con criterio questi operatori, è possibile ottenere risultati più mirati, pertinenti e completi.

Per comprendere la potenza di queste tecniche si possono esaminare esempi pratici:

- inurl:phpbb1.txt
- xamppdirpasswd.txt filetype:txt
- Instagram password filetype:txt
- site:clusit.it filetype:pdf
- site:uniroma2.it filetype:xls

# Motori di ricerca: Bing

Non esiste un unico motore di ricerca affidabile: ampliare il proprio orizzonte e sperimentare soluzioni alternative a Google può incrementare notevolmente le possibilità di individuare informazioni utili.

Bing, spesso considerato il “fratello minore” di Google, gestisce comunque almeno il 20% delle ricerche mondiali e offre alcuni operatori esclusivi. Ad esempio, “**linkfromdomain**:” restituisce le pagine raggiungibili dai link di un determinato dominio, mentre “**ip**:” permette di individuare tutti i siti ospitati da uno specifico indirizzo IP, una funzione utile per scoprire quali siti risiedano sullo stesso server.

Altri operatori di Bing, come “**contains**:” e “**filetype**:”, semplificano la ricerca di documenti di un formato ben preciso (PDF, musica, video). Inoltre, l’uso di “**loc**:” o “**location**:” consente di filtrare i risultati in base al Paese d’origine delle pagine, potendo anche specificare la lingua tramite “**language**:”. Ad esempio, “Software Company” loc:in limita la ricerca alle aziende software in India, mentre “MSOFTX” loc:cn language:en cerca contenuti pertinenti allo switch MSOFTX di Huawei localizzati in Cina ma scritti in inglese.

Infine, operatori come “**feed**:” e “**hasfeed**:” facilitano l’individuazione di feed RSS o Atom, offrendo un ulteriore livello di approfondimento.

## Motori di ricerca: Baidu

Baidu, considerato il terzo motore di ricerca più grande al mondo e il primo in Cina, supporta molti degli operatori standard utilizzati in altri motori, offrendo così una certa familiarità nell’approccio all’indagine. Gli operatori site:, domain:, inurl:, allinurl:, intitle:, allintitle: e filetype: sono tutti utilizzabili in Baidu per affinare la ricerca e filtrare i risultati in base alle specifiche esigenze dell’analista. Inoltre, Baidu dispone di versioni locali, come (http://www.baidu.jp) o edizioni dedicate a Paesi quali Thailandia ed Egitto, permettendo di accedere a informazioni targettizzate su determinate aree geografiche. Questa versatilità rende Baidu uno strumento prezioso per chi conduce ricerche OSINT a livello globale, soprattutto in contesti linguistici e culturali diversi da quelli anglofoni.

## Motori di ricerca: Yandex

Yandex, il motore di ricerca più popolare in Russia, offre funzionalità avanzate e operatori personalizzati che consentono di ottenere risultati altamente mirati. Ad esempio, è possibile filtrare i risultati in base al tipo di file utilizzando l’operatore **mime=**, seguito dal formato desiderato, come html, pdf, doc, ppt, xls, rtf o swf. Questo permette di individuare rapidamente documenti e contenuti specifici all’interno del web.

Inoltre, Yandex consente di restringere la ricerca a domini appartenenti a determinate aree geografiche o istituzionali. Con l’operatore **rhost:**, seguito da un TLD (Top-Level Domain), si può visualizzare l’insieme dei siti indicizzati. Ad esempio, **rhost:ro.*** permette di consultare tutti i siti con dominio .ro; analogamente, **rhost:edu.*** mostra tutti i siti con dominio .edu. Combinando quest’ultimo operatore con **inurl:**, è possibile affinare ulteriormente la ricerca: _*rhost:edu.* inurl:ftp_* restituirà solo i siti .edu che contengono “ftp” all’interno dell’indirizzo.

Un altro punto di forza di Yandex è la possibilità di filtrare i risultati in base alla lingua dei contenuti, grazie all’operatore **lang=**. Con lang=”ru” si visualizzano pagine in russo;

lang=”uk” restringe la ricerca all’ucraino; lang=”be” al bielorusso; lang=”en”, lang=”fr” e lang=”de” permettono invece di esplorare contenuti in inglese, francese e tedesco. Ad esempio, la query **ballistics lang=”uk”** mostrerà solo i risultati in lingua ucraina relativi alla parola “ballistics”.

Queste funzioni permettono all’analista OSINT di ampliare il raggio di ricerca, individuando risorse utili non solo in contesti geografici e culturali diversi, ma anche in formati e lingue specifiche.

## Meta Search Engine

I motori di ricerca “metasearch” non indicizzano direttamente il web, ma si appoggiano a una pluralità di motori tradizionali, aggregando i risultati ottenuti. Questo approccio permette di ottenere una panoramica più ampia e diversificata di ciò che è disponibile online, riducendo la necessità di ripetere manualmente le stesse query su piattaforme differenti. Esempi di metasearch engine includono All-in-One, AllTheInternet, Etools, FaganFinder, Goofram, iZito, Nextaris, Metabear, Myallsearch, Qwant, Sputtr, Trovando, WebOasis e Zapmeta. Questi servizi forniscono un punto di accesso unico a molteplici fonti, agevolando il compito di chi conduce ricerche e analisi OSINT, in quanto consentono di individuare velocemente risorse e informazioni provenienti da svariati database online.

## Elenchi Telefonici

Gli elenchi telefonici rappresentano un’altra risorsa da non sottovalutare nel campo delle ricerche OSINT. Oltre ai classici servizi come le pagine gialle e le pagine bianche, è possibile trovare utili riferimenti negli elenchi interni di aziende, università e altre istituzioni, spesso messi a disposizione sui relativi siti web. Esistono anche elenchi telefonici internazionali consultabili online, come http://www.infobel.com e http://www.paginebianche.it/.

Un buon analista OSINT dovrebbe mantenere una propria lista aggiornata di queste risorse, poiché vengono rinnovate con frequenza. Tenere traccia degli elenchi più completi e affidabili, e monitorare periodicamente la disponibilità di nuovi servizi e aggiornamenti, può fare la differenza nel reperire informazioni utili e verificabili.

# Analisi delle immagini

I dati EXIF (Exchangeable Image File Format) possono fornire molte informazioni utili su una fotografia. Tra queste, è possibile identificare la fotocamera utilizzata, insieme a dettagli tecnici relativi alle caratteristiche della foto, come impostazioni di esposizione, apertura e ISO. Questi dati possono essere utilizzati, ad esempio, per collegare una fotografia a una determinata macchina fotografica o addirittura a un utente specifico.

Inoltre, i dati EXIF spesso includono informazioni su data e ora dello scatto, oltre alla localizzazione geografica (se il dispositivo è dotato di GPS). Queste informazioni possono rivelarsi preziose per analisi tecniche o contestualizzazioni.

Esistono numerosi strumenti, anche online, per visualizzare i dati EXIF di una foto. Uno di questi è un'estensione per il browser Firefox, chiamata "EXIF Viewer", disponibile al seguente link: https://addons.mozilla.org/it/firefox/addon/exif-viewer/.

Tuttavia, è importante sottolineare che la maggior parte dei siti web, come Facebook e altre piattaforme social, rimuovono tutti i dati EXIF dalle immagini caricate, con particolare attenzione alla rimozione dei dati GPS per motivi di privacy.

Inoltre, la ricerca per immagini permette di ottenere una vasta gamma di informazioni che vanno ben oltre i dati EXIF di una foto. Analizzando un'immagine, si possono trarre dettagli sull'ambiente circostante, le persone presenti, la situazione rappresentata e il contesto generale. Inoltre, è possibile investigare dove l'immagine è stata trovata, ad esempio su un sito web, un social network o altre piattaforme.

Una delle tecniche più potenti è la ricerca inversa per immagini, che consente di scoprire altre informazioni disponibili online. Questa funzione permette di individuare copie o versioni dell'immagine in rete e, in alcuni casi, di risalire alla sua origine o al primo utilizzo.

Un aspetto cruciale da considerare è che l'uso di un'immagine trovata online, ad esempio per creare un profilo falso, può essere facilmente smascherato. Strumenti come **Tineye** sono estremamente efficaci nel rintracciare l'immagine originale e rivelare eventuali manipolazioni.

Infine, servizi specializzati come **Stolen Camera Finder** possono essere utilizzati per rintracciare fotocamere rubate, sfruttando i dati seriali presenti nei file delle immagini. Questi strumenti offrono un valore aggiunto per chi cerca di proteggere i propri dispositivi o identificare l'origine di una fotografia.

---

**Esempio.** Dato il seguente post su Twitter


Per verificare l’esattezza dell’informazione in esso contenuta, si possono seguire alcune procedure ben definite. Innanzitutto, è necessario individuare le geo-coordinate dell’aeroporto di Latakia, noto anche come Aeroporto Bassel Al-Assad, consultando la pagina Wikipedia relativa. Da questa pagina è possibile ottenere le coordinate geografiche esatte.

Una volta ottenute le coordinate, si può cliccare su di esse per accedere a strumenti che consentono di visualizzare l’area su diverse piattaforme di mappe, come Google Maps o OpenStreetMap. Questo permette di confrontare le caratteristiche della pista dell’aeroporto, come linee, marcature o il layout generale, con quelle visibili nella foto oggetto di analisi.

Un altro passo importante è l’analisi del paesaggio. Si osservano elementi geografici come colline o altri dettagli visibili nella foto per confrontarli con le immagini satellitari disponibili, verificando che corrispondano all’area circostante l’aeroporto. È inoltre utile individuare particolari distintivi, come edifici, infrastrutture o elementi visibili, ad esempio un’antenna radar, e confrontarli con le immagini satellitari per verificarne la corrispondenza.

Infine, si può tentare di identificare il tipo di aerei raffigurati nella foto, analizzandone le sagome o altre caratteristiche riconoscibili e confrontandole con database o immagini online di modelli conosciuti, come i caccia russi Sukhoi.

Questa serie di passaggi consente di verificare se la foto sia effettivamente stata scattata presso l’aeroporto indicato e di confermare o smentire l’autenticità delle informazioni fornite. Se desideri approfondire uno di questi aspetti o necessiti di supporto per una ricerca specifica, fammi sapere.

# Maritime OSINT

La Maritime OSINT sfrutta fonti aperte per raccogliere informazioni su navi, rotte marittime, porti e altre attività correlate. Per trovare informazioni e tracciare le navi, è utile concentrarsi su dati chiave come il nome della nave, il numero IMO (International Maritime Organization), il codice MMSI (Maritime Mobile Service Identity), la bandiera della nave e la sua ultima posizione conosciuta. Utilizzando piattaforme specializzate, è possibile ottenere informazioni in tempo reale grazie al sistema AIS (Automatic Identification System). Questi strumenti consentono di monitorare il tipo di nave, analizzare le rotte passate e verificare le informazioni raccolte.

Tra le risorse utili, VesselFinder fornisce tracciamento AIS in tempo reale con dati dettagliati. Maritime Connector è ideale per reperire informazioni su equipaggi e mercati. MarineTraffic offre monitoraggio in tempo reale e accesso allo storico delle rotte, mentre ShipFinder è una soluzione semplice per il monitoraggio AIS. Integrando i dati raccolti con strumenti come Google Earth o database governativi, è possibile ampliare l'analisi e verificare certificazioni o incidenti. È importante rispettare la normativa sulla protezione dei dati personali, come il GDPR.

# Wayback Machine

Il detto "Internet non dimentica" ha un fondo di verità grazie a strumenti come la Wayback Machine. Questo progetto, parte di Archive.org, si propone di archiviare pagine web e tracciare le loro modifiche nel tempo. È uno strumento prezioso per recuperare informazioni che potrebbero essere state cancellate o modificate nel web attuale.

Grazie alla Wayback Machine, è possibile accedere a vecchie versioni di siti web, recuperare rubriche telefoniche, dati storici o contenuti che non sono più disponibili. Questi dati, una volta recuperati, possono essere analizzati e confrontati con quelli attuali, offrendo spunti interessanti per ricerche, indagini e studi storici sul web.

Il sito più conosciuto per questo scopo è Archive.org, che rappresenta una risorsa centrale per chiunque voglia esplorare la memoria digitale di Internet.

# Social Network: Twitter

Twitter, con milioni di utenti attivi, rappresenta una fonte immensa di informazioni utili per varie tipologie di analisi e ricerche. La piattaforma identifica ogni profilo tramite il carattere “@”, che precede il nome utente, e consente la creazione di account senza l’obbligo di usare un nome reale, anche se sono necessari un'email e un numero di telefono per la registrazione.

La ricerca delle informazioni su Twitter è resa semplice ed efficace grazie al suo motore di ricerca interno. È possibile accedere al box di ricerca presente nella pagina principale o utilizzare i form specifici disponibili nelle pagine dedicate, come quelle di ricerca avanzata. In

alternativa, è possibile costruire URL personalizzate per ricerche mirate, includendo le parole chiave desiderate direttamente nella stringa dell'indirizzo.

Tra i principali strumenti disponibili ci sono:

- La pagina iniziale di ricerca, accessibile all'indirizzo https://twitter.com/search-home.
- La ricerca avanzata, che consente di filtrare i risultati in base a criteri specifici, disponibile su https://twitter.com/search-advanced.
- La possibilità di utilizzare URL ad hoc, come ad esempio https://twitter.com/search?q=keywords, sostituendo "keywords" con le parole chiave di interesse.

Twitter offre una serie di funzionalità di ricerca e analisi che possono essere ulteriormente ampliate con strumenti esterni. Utilizzando il box di ricerca interno, è possibile filtrare i risultati secondo diverse categorie, tra cui popolari, più recenti (ultime due settimane), persone, foto, video, notizie e trasmissioni live (ad esempio tramite Periscope).

Per analizzare i profili, Twitter fornisce URL strutturati che consentono di accedere a informazioni specifiche:

- Per visualizzare i like di un utente: `twitter.com/username/likes`
- Per i follower: `twitter.com/username/followers`
- Per gli account seguiti: `twitter.com/username/following`
- Per i media condivisi: `twitter.com/username/media`
- Per le risposte ai tweet: `twitter.com/username/with_replies`
- Per le liste: `twitter.com/username/lists`

Oltre alle funzionalità native, esistono strumenti di terze parti che utilizzano le API di Twitter per offrire funzionalità avanzate. Tra questi troviamo:

- **One Million Tweet Map**: visualizza i tweet in tempo reale su una mappa.
- **Twitterfall**: consente di seguire flussi di tweet basati su parole chiave.
- **Tinfoleak**: uno strumento di OSINT che analizza account Twitter e fornisce informazioni dettagliate come i dispositivi utilizzati, le geolocalizzazioni, i tweet visualizzati in Google Earth, e statistiche sui hashtag, menzioni e argomenti trattati.

Altri strumenti utili includono:

- **Followerwonk**: analizza i follower e il comportamento degli utenti.
- **GeoSocial Footprint**: mappa la geolocalizzazione delle attività.
- **OmniCity**: fornisce analisi dettagliate sui profili Twitter.
- **Mentionmapp**: visualizza una mappa delle menzioni e interazioni.
- **Twitonomy**: offre statistiche approfondite sugli account Twitter, come la frequenza dei tweet e le analisi di engagement.

Questi strumenti sono particolarmente utili per la raccolta e l'analisi di dati a fini investigativi, di ricerca o di monitoraggio dei social media.

# Social Network: Instagram

La ricerca su Instagram può essere effettuata direttamente tramite il box di ricerca che include una funzione di autocompletamento. Oltre alla ricerca nativa, esistono servizi esterni che facilitano l'esplorazione del contenuto pubblico sulla piattaforma. Tra questi:

- Imgrum: permette ricerche per parole chiave.
- Tofo.me: fornisce una visualizzazione di profili e post.
- Mininsta: consente l'esplorazione di profili e contenuti.
- Websta: offre analisi e ricerca sui contenuti di Instagram.
- The Picta: facilita la navigazione nei contenuti.

Per analizzare connessioni e interazioni come i "like", è possibile integrare questi strumenti con i motori di ricerca tradizionali.

# Social Network: Facebook

Ogni elemento su Facebook, come profili, post, foto o commenti, è un oggetto referenziato in un database con un ID numerico univoco. Questo ID consente di mettere in relazione gli oggetti e di eseguire ricerche mirate.

## Individuare l'ID di un profilo o di un oggetto

Per individuare un User ID o l'ID di altri oggetti, si possono usare strumenti online come:

- Find My FB ID
- Lookup ID
- SEO Tool Station

Analizzando le URL delle foto, l'ID può essere individuato direttamente. Ad esempio, in una URL come: `https://www.facebook.com/photo.php?fbid=10154851531324251&set=pb.725584250.-2207520000.1467299078.&type=3&theater`, l'ID è rappresentato dal numero accanto a `fbid`.

## Usare l'ID per accedere a un profilo

Con un User ID, si può accedere al profilo corrispondente con URL come:

- `https://www.facebook.com/[ID]`
- `https://www.facebook.com/profile.php?id=[ID]`

## Ricerche con Facebook Graph Search

Facebook Graph Search, introdotto nel 2013, permette di effettuare query dettagliate sul database della piattaforma. Attraverso il box di ricerca, si possono cercare parole chiave, categorizzare i risultati e perfezionarli ulteriormente con filtri. Tuttavia, dopo ottobre 2019, Facebook ha limitato molte di queste funzionalità, rendendo le ricerche più complesse.

## Strumenti esterni per ricerche su Facebook

Per ovviare alle limitazioni di Graph Search, si possono utilizzare strumenti esterni come:

- Gist Facebook Search Tool
- Sowdust Facebook Search
- Go Find Who
- Aware Online Facebook Search Tool
- Graph Tips
- Who Posted What
- Intelx Facebook Tools
- Search is Back
- Facebook Matrix

Questi strumenti permettono di esplorare i dati pubblici su Facebook in modo più approfondito e mirato, compensando le limitazioni introdotte da Facebook stesso.

# Analisi delle fonti

L'analisi e la valutazione delle fonti rappresentano un aspetto cruciale nel processo di raccolta e verifica delle informazioni in ambito OSINT. Per determinare l'affidabilità delle fonti, è necessario rispondere a cinque domande chiave: Who, When, Where, What, e Why.

**Who** riguarda l'autore dell'informazione. È importante identificare chi ha creato il contenuto, verificando se si tratta di una fonte autorevole con una buona reputazione. La verifica delle pubblicazioni precedenti e del loro giudizio da parte di altri contribuisce a stabilire la credibilità della fonte.

**When** si concentra sul momento della pubblicazione. È essenziale definire chiaramente la data e il contesto in cui l'informazione è stata diffusa, poiché la sua attualità e rilevanza possono influenzare la qualità dell'analisi.

**Where** analizza il luogo di pubblicazione. Valutare l'affidabilità del sito o della pagina web e determinare se si tratta di una fonte pubblica o privata è fondamentale. Inoltre, il contesto geografico o il dominio del sito possono fornire ulteriori indizi sulla sua attendibilità.

**What** esamina il contenuto stesso dell'informazione. È necessario verificare se è supportato da altre fonti indipendenti, il che può contribuire a confermare o smentire la validità dei dati raccolti.

**Why** si interroga sulle motivazioni dietro la pubblicazione dell'informazione. Comprendere gli scopi, gli interessi o le intenzioni dell'autore può aiutare a individuare eventuali bias o manipolazioni.

L'approccio sistematico a queste domande garantisce un'analisi approfondita e consente di separare informazioni valide da quelle potenzialmente fuorvianti, migliorando la qualità del processo decisionale basato sui dati raccolti.

# OSINT Report

Un report OSINT deve essere un documento chiaro e completo, capace di comunicare le informazioni raccolte in modo strutturato e comprensibile. Deve includere un riepilogo sintetico (executive report) pensato per i non specialisti, riportare le fonti utilizzate, descrivere le metodologie adottate durante la ricerca e, se possibile, suggerire ulteriori direzioni da esplorare.

Per esempio, un report OSINT su una persona può contenere informazioni personali e familiari, immagini del soggetto, interessi e hobby, contatti come email, numeri di telefono, indirizzi o profili social, dati accademici, lingue conosciute, esperienze professionali, occupazione attuale, collaborazioni lavorative, associazioni e persone di rilevante importanza. Inoltre, possono essere inclusi collegamenti a materiali e documenti rilevanti e annotazioni specifiche dell’operatore.

Per la documentazione delle prove, è essenziale acquisire le informazioni mostrate nelle pagine web in un modo che garantisca l'integrità e la verificabilità temporale. Una pagina web, ad esempio, può essere salvata e firmata digitalmente per includere data e ora dell'acquisizione. Strumenti come **Hashbot** permettono di acquisire contenuti web e applicare firme digitali verificabili. FAW, il primo browser progettato per l'acquisizione forense delle pagine web, fornisce un ambiente dedicato per raccogliere dati con una validità forense. X1 Social Discovery è un altro strumento potente per raccogliere informazioni da social media, fornendo un'analisi avanzata.

Se non è necessaria una firma digitale, strumenti più semplici come PrintFriendly possono essere utilizzati per generare versioni salvabili o stampabili di pagine web. In ogni caso, l’utilizzo di strumenti adeguati dipende dal contesto e dagli obiettivi del report OSINT, garantendo sempre un approccio rigoroso e documentato.