CSCORZA

Manuale Basico di Open Source Intelligence

MANUALE BASICO DI

OPEN SOURCE INTELLIGENCE

Testo scritto e prodotto da **CScorza**

Anno di pubblicazione 2024

Contatti:

Linkedin : https://www.linkedin.com/in/cscorza
Twitte/X: https://x.com/CScorzaOSINT
Telegram: https://t.me/CScorzaOSINT - *"CScorza – Indagini Telematiche"*
GitHub: https://github.com/CScorza
LAB4INT: https://www.lab4int.org

INDICE

PREFAZIONE

È con grande piacere e onore che presento questo "Manuale Basico di Open Source Intelligence" scritto da CScorza. Ho avuto il privilegio di conoscere personalmente CScorza durante il corso di Digital Intelligence, dove ha dimostrato non solo una professionalità e competenza straordinarie, ma anche una notevole attitudine nella divulgazione delle proprie conoscenze sull'OSINT e sull'anonimato, principio fondamentale delle indagini sotto copertura.

CScorza ha realizzato un lavoro encomiabile, creando un manuale che si rivolge sia ai neofiti che agli esperti del settore. La sua capacità di trasformare concetti complessi in informazioni accessibili e utili è una testimonianza del suo impegno e della sua passione per l'argomento. Questo manuale non è solo una raccolta di tecniche e strumenti, ma una guida pratica e teorica che fornisce una panoramica completa dell'OSINT, dalle basi storiche alle applicazioni più avanzate.

Il manuale esplora in dettaglio le diverse branche dell'OSINT, come la Social Media Intelligence (SOCMINT), e molte altre. Attraverso capitoli ben strutturati, CScorza ci guida nella creazione di workstation dedicate, nell'uso di VPN e password manager, e nell'analisi avanzata degli user agent. La sezione sulla creazione di avatar per l'infiltrazione nei social network è particolarmente utile per chi desidera approfondire le tecniche di anonimato e protezione dell'identità.

La raccolta e l'analisi delle informazioni da fonti pubblicamente disponibili sono oggi più cruciali che mai. Viviamo in un'epoca in cui la quantità di dati accessibili è enorme, e la capacità di estrarre informazioni utili da questo mare di dati è una competenza essenziale. CScorza, con questo manuale, ci offre gli strumenti e le conoscenze necessarie per navigare in questo complesso panorama informativo.

Voglio sottolineare che l'OSINT è un campo in continua evoluzione. Le tecniche e gli strumenti che oggi consideriamo all'avanguardia potrebbero rapidamente diventare obsoleti. Pertanto, l'apprendimento continuo e l'aggiornamento costante sono essenziali. Questo manuale rappresenta un punto di partenza fondamentale per chiunque voglia intraprendere questo percorso, ma non deve essere considerato un punto di arrivo.

In conclusione, elogio il lavoro di CScorza per la sua dedizione e per aver messo a disposizione di tutti noi le sue competenze. Sono sicuro che questo manuale diventerà un riferimento prezioso per molti operatori del settore.

Benvenuti nel mondo dell'Open Source Intelligence!

Dr. Simone Bonifazi
Presidente di LAB4INT

INTRODUZIONE

Se ti stai battendo in questo manuale, vuol dire che già mi conosci e segui i miei canali Telegram oltre alla mia pagina GitHub, dove con gli anni ho messo insieme una serie di repository che racchiudono tutti gli strumenti utili per la navigazione sul web, per la raccolta e l'analisi OSINT in molte delle sue sottoclassi (es. SOCMINT, GEOINT, CORPINT etc.), Digital Forensics e l'OSINT Image, ovvero l'analisi delle immagini per la raccolta delle informazioni che possono esserci utili per raggiungere il nostro obiettivo. Data l'incessante richiesta di creare qualcosa che possa aiutare anche chi è alle prime armi nel mondo dell'OSINT, ho iniziato a scrivere e mettere insieme questo manuale, al fine di cogliere i punti salienti per la creazione di una "*workstation basic*", quindi una serie di strumenti che vanno non solo dall'hardware al software, ma anche le tecniche ed i consigli per iniziare il nostro monitoraggio, raccolta ed analisi delle informazioni accessibili su internet.

Iniziamo con due domande:

Serve un manuale di OSINT? e che cos'è l'OSINT?

Per rispondere alla prima domanda, dobbiamo per forza partire dalla seconda. L'OSINT, ovvero l'Open Source Intelligence, è la raccolta e l'analisi di informazioni da fonti disponibili pubblicamente per supportare processi decisionali e operazioni d'intelligence. Per la sua natura, si presta a scenari di natura governativa (forze dell'ordine, forze armate e servizi d'intelligence) e contesti privati.

La capacità di un buon analista consiste nel trasformare semplici dati, che apparentemente possono sembrare banali, in informazioni significative. Pertanto, tale processo viene racchiuso nel ciclo dell'intelligence, di cui parleremo nei prossimi capitoli. L'efficacia di una buona analisi dipende dall'abilità dell'operatore di identificare, accedere ed analizzare fonti ed informazioni aperte, garantendo accuratezza e pertinenza dei dati raccolti. A questo punto alla domanda, se "serve un manuale di OSINT", la risposta è "ni", perché non esiste una linea guida che vada bene per qualsiasi analista, in quanto ogni operatore ha un suo bagaglio culturale fatto di conoscenze, capacità informatiche ed intelligence che lo possono aiutare e supportare durante l'attività. Inoltre, ogni Stato, ha diversi regolamenti che riguardano il diritto alla *privacy* ed il trattamento dei dati personali, per questo un buon operatore, si aggiorna e studia i vari luoghi dove sta affrontando le proprie ricerche, per trovare i suoi dati su database pubblici, i social

network più diffusi in una determinata area geografica come, per esempio, WeChat per la Cina o Ok, VKontakte per la Russia, etc.

È pur vero che bisogna partire da delle basi, ed ecco qui che mi sono cimentato a scrivere qualcosa che sia di facile uso per chiunque entri in questo mondo.

Altro elemento da tenere in considerazione è il Big Data. Ad oggi ogni operatore è sommerso da centinaia di informazioni, e sta appunto all'abilità di quest'ultimo decidere cosa considerare come dato utile per poi inserirlo nel proprio report e cosa no. L'OSINT in questo ci dà degli strumenti utili e necessari per riuscire ad eliminare quello che viene definito "rumore" ovvero informazioni fuorvianti, facendo emergere solo quelli che sono destinati ad essere inseriti nel nostro report finale.

Questo manuale nasce dai corsi e dalle esperienze acquisite nel corso degli anni nel campo dell'OSINT. Poiché questo settore è estremamente dinamico, l'aggiornamento continuo è essenziale. Perciò, questo manuale non rappresenta la fine del vostro percorso, ma piuttosto un punto di partenza o un ulteriore passo avanti nella vostra continua ricerca di informazioni.

A questo punto, Benvenuti nel mondo dell'Open Source Intelligence!!!

1. STORIA DELL'OSINT E TUTTE LE SUE BRANCHE

Le prime forme di raccolta informativa possono essere rintracciate nelle antiche civiltà, dove gli addetti alle strategie belliche (governanti e generali), si affidavano a mercanti, viaggiatori e diplomatici per ottenere informazioni strategiche. Romani e Greci, per esempio, si servivano di queste informazioni per la pianificazione delle campagne militari.

Durante il Medioevo, la raccolta delle informazioni continuò, con l'unione di cronache locali, resoconti di viaggi e lettere di missionari e mercanti. Loro, infatti, erano i conoscitori di territori lontani e potevano aiutare a comprendere le dinamiche politiche e sociali delle diverse regioni.

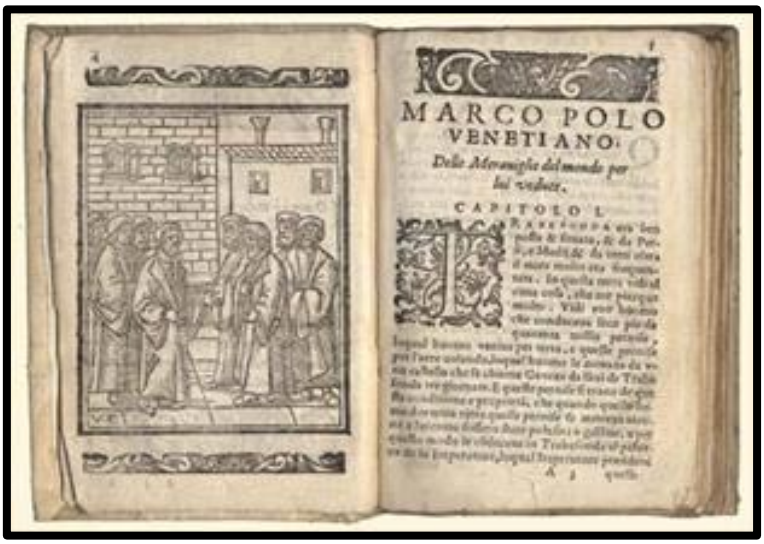

MARCO POLO
VENETIANO.
Delle Meraviglie del mondo per lui vedute.
CAPITOLO I.

Figura 1:- Il Milione

Con l'avvento della stampa in età moderna, tali notizie crebbero esponenzialmente, i giornali divennero una fonte cruciale di informazioni per governi ed organizzazioni militari, permettendo di monitorare eventi nelle varie regioni e sviluppi tecnologici e politici.

Durante le due Guerre Mondiali, l'uso di strumenti per la ricerca d'informazioni si intensificò notevolmente. Tramite attività come il SIGINT (intercettazioni delle trasmissioni radio), la stampa straniera e altre fonti pubbliche, era possibile raccogliere informazioni strategiche. I governi utilizzavano la propaganda e la contro-propaganda per influenzare l'opinione pubblica.

Figura 2:- Il Secret Intelligence Service (S.I.S.)

Figura 3:- Lo Sicherheitsdienst

Figura 4:- L'Office of Strategic Services (O.S.S.) USA

La guerra fredda fu caratterizzata da una competizione ideologica, militare ed economica tra l'occidente guidato dagli USA e l'oriente guidato dall'URSS. In questo contesto la raccolta informativa giocò un ruolo cruciale per le strategie d'intelligence delle due superpotenze. Anche se le informazioni sull'avversario erano molto limitate, ciò che poteva essere d'aiuto era sicuramente l'uso di fonti di accesso pubblico, come la raccolta e l'analisi sulla politica e sulla sicurezza.

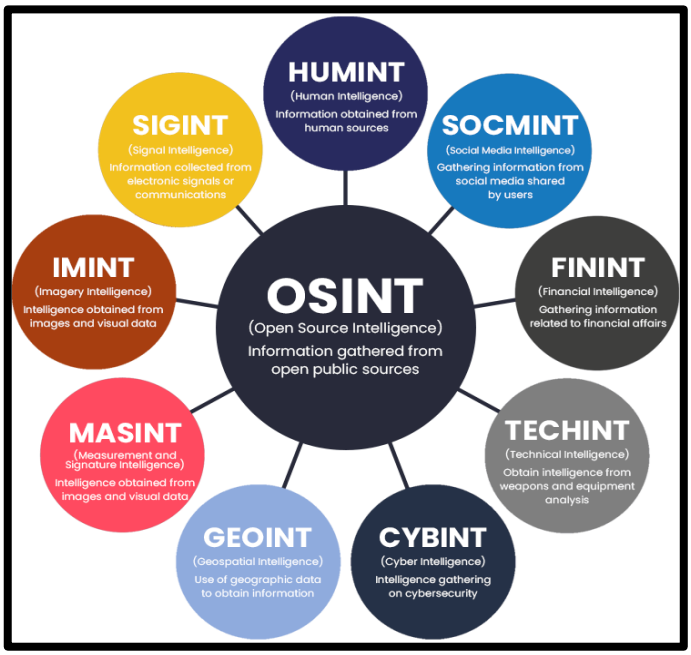
Figura 5:- KGB Comitato per la sicurezza dello Stato - URSS

Figura 6:- CIA Central Intelligence Agency- US

Con l'era digitale e la rivoluzione delle comunicazioni, la quantità d'informazioni è esplosa, includendo, forum, siti web, social media e blog. In questo contesto, la possibilità di accedere ad una vasta gamma di dati in tempo reale ha trasformato radicalmente la capacità di raccolta e analisi. Grazie a strumenti di scraping, data mining e analisi dei social media si è resa l'attività di OSINT più efficiente e precisa. Con questi strumenti possiamo raccogliere, filtrare ed analizzare grandi quantità di dati. L'importanza dell'OSINT ha investito anche interessi privati in quanto possono essere utili per vari scopi, come la

sicurezza delle proprie infrastrutture, l'analisi dei rischi e quindi la protezione di eventuali minacce. I sottogruppi che fanno capo all'OSINT sono:

- SOCMINT – *Social Media Intelligence*
- GEOINT – *Geospatial Intelligence*
- IMINT – *Image Intelligence*
- VATINT – *Vehicle and Transportation Intelligence*
- SIGINT – *Signals Intelligence*
- TECHINT – *Tecnical Intelligence*
- FININT – *Financial/Bussiness Intelligence*
- TRADINT – *Corporate Intelligence*
- HUMINT – *Human Intelligence*
- SE – *Social Engineering*
- MASINT – *Measurement ad Signature Intelligence*
- DNINT – *Digital Network Intelligence*
- RUMINT – *Rumor Intelligence*
- OPSEC – *Operation Security*
- TSCM – *Technical Surveillance – Counter- Measures*
- CI – *Counter – Inteligence/Confidential Informat*
- POI - *Person of Interest*.



L’insieme di questi sottogruppi, fanno sì che la ricerca di informazioni venga suddivisa per settore di competenza e per conoscenza dell’argomento. Tutti quanti però rispondo a quattro fasi distinte:

- Scoperta (*Discovery*) – Sapere chi sa (*Know who knows*)
- Individuazione (*Discrimination*) – Sapere “cosa è cosa” (*Know What’s What*)
- Distillazione (*Distillation*) – Sapere cosa è "rilevante" (*Know What’s hot*)
- Disseminazione (*Dissemination*) - Sapere “chi è chi” (*Know Who’s Who*)

Questo perché con l’era digitale le “informazioni” su una singola notizia sono molteplici. Quindi diventa importante saper distinguere i “dati” veri da quelli falsi, oppure quelli importanti ai fini investigativi da quelli di meno d’interesse operativo.

2. OSINT ATTIVO E OSINT PASSIVO (MONITORAGGIO)

È importante distinguere queste due attività al fine di non cadere in inganno durante la raccolta delle informazioni. Difatti in base al livello di grado di interazione che possiamo avere con il target, possiamo trovarci ad operare una diversa tipologia di attività.

Di seguito abbiamo quindi:

- **OSINT PASSIVO**

  Consiste in un monitoraggio e raccolta di informazioni su uno specifico target o gruppi, senza alcuna interazione. Ovvero vi è una raccolta di dati che sono già disponibili pubblicamente senza lasciare tracce della propria presenza o attività.

Un esempio può essere:

- **il monitoraggio di un profilo Facebook:** raccogliendo foto, commenti, informazioni personali etc., senza lasciare un like, un commento o condividere un post presente nella bacheca del target;
- **analisi di un sito web o di un blog:** lettura di articoli, blog senza che il proprietario del sito sia a conoscenza di chi sta visitando il sito;
- **ricerca database pubblici:** accesso a registri pubblici, archivi o altri database che non richiedono interazioni con la fonte.

- **OSINT ATTIVO**

  In questa fase, vediamo che una forma di interazione con le fonti di informazioni è presente.

  Per esempio, la creazione di un profilo fake o avatar (che affronteremo più avanti), può essere utile al fine di registrarsi su un social network, forum o anche l'invio di e-mail per accedere a informazioni generiche che non siano indirettamente collegate all'attività criminale.

  L'OSINT Attivo non deve essere però confuso con l'attività Undercover o agente sotto copertura, che è disciplinato da un'altra norma rispetto alla raccolta delle fonti di prova e che richiede tutta una serie di operazioni preliminari specifiche per questo tipo di attività.

3. PROCESSI DEL FLUSSO DI LAVORO OSINT - "METODO PIVOTING"

Nell'indagine digitale, una delle domande più comuni è:

"Esiste un processo o flusso di lavoro standard per OSINT, SOCMINT e la raccolta dati in generale?"

Per rispondere a questa domanda, dovremmo tenere conto del fatto che ogni indagine è unica, lo scenario del cyberspazio è estremamente dinamico (ad esempio un utente finale o un social media che cambia frequentemente le sue politiche sulla *privacy*) e nessun "*cheat sheet*" può essere utilizzato per ogni caso. Quindi, potrebbe essere un azzardo rispondere "*Sì*" alla domanda di cui sopra. Ad ogni modo, possiamo utilizzare una sorta di soluzione basata su mappe mentali, che può aiutare rapidamente con direzione e guida.

Questa soluzione prende in considerazione sei categorie in base alle informazioni ricercate, come:

- **E-mail;**
- **Nome utente o username;**
- **Numero di telefono;**
- **Nome di dominio;**
- **Geolocalizzazione.**

Ciascuno dei seguenti flussi di lavoro dovrebbe essere considerato quando stiamo ricercando un argomento scelto. Per esempio:

- Se ci viene fornito un indirizzo e-mail, il nostro obiettivo è trovare eventuali nomi utente e nomi reali;
- Quando abbiamo un nome utente, il nostro obiettivo è trovare eventuali social network e verificare un indirizzo e-mail;
- Quando abbiamo un nome vero, l'obiettivo è trovare indirizzi e-mail, nomi utente e numeri di telefono;
- Quando abbiamo un numero di telefono, il nostro obiettivo è verificare il nome e identificare un indirizzo fisico e parenti;
- Quando abbiamo un nome di dominio, il nostro obiettivo è individuare un nome e un indirizzo reale;

Il ciclo continua dopo che viene scoperta ogni nuova informazione.

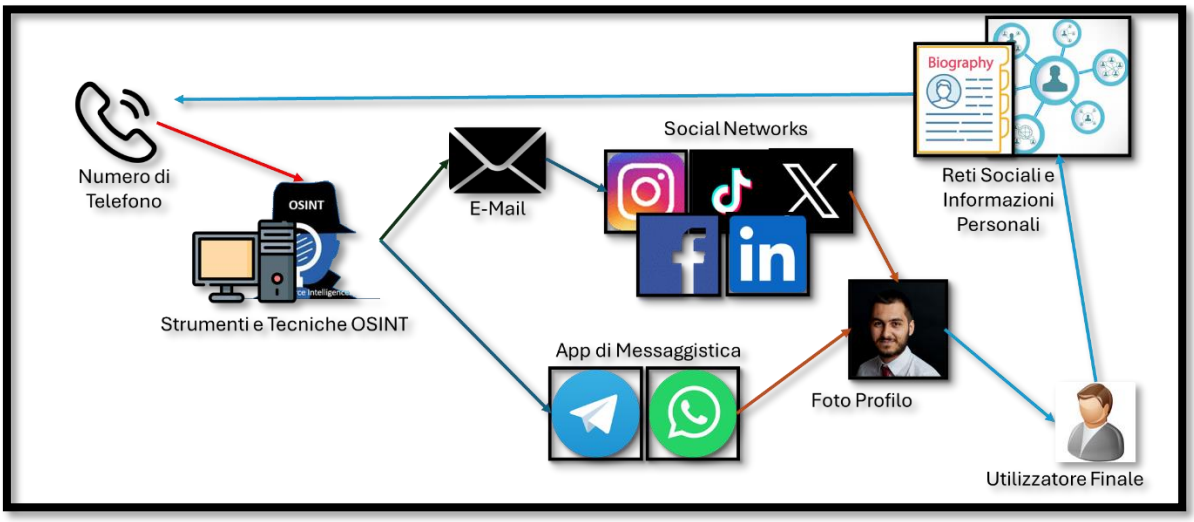


Figura 7:- Esempio di Attività OSINT

3.1. METODO PIVOTING

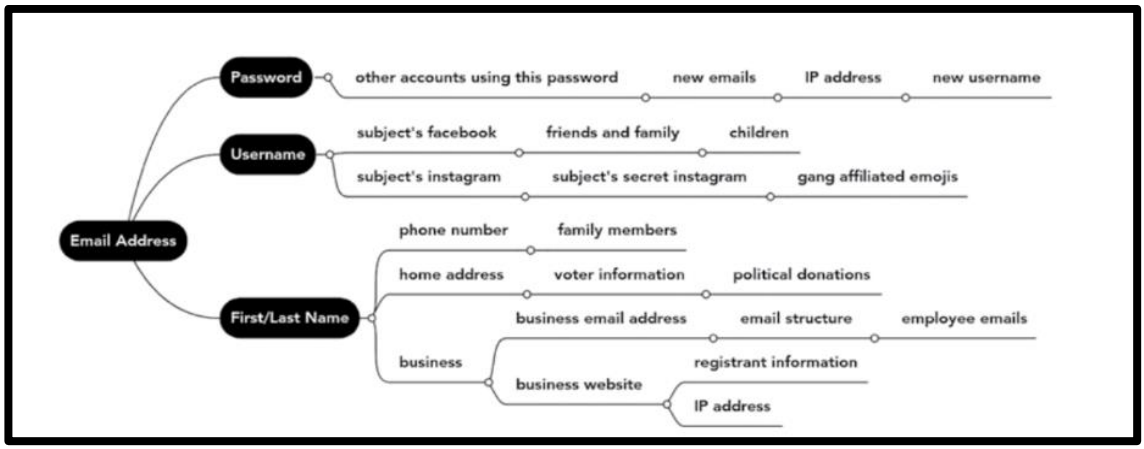


Figura 8:- Tratto dal libro DeepDive di Biker Wiley

Il ciclo che abbiamo fin qui descritto prende il nome di "*Metodo Pivoting*" e si realizza creando delle flowchart che servono al singolo operatore a creare una sorta di linea guida nelle prime fasi del ciclo dell'intelligence[1] ovvero la raccolta delle informazioni.

[1] Dal punto di vista della funzione, l'intelligence può essere descritta come processo informativo definito da un ciclo di azioni articolato in più fasi (cosiddetto "ciclo intelligence") finalizzato agli obiettivi generali individuati dalle autorità di governo (*https://www.sicurezzanazionale.gov.it/cosa-facciamo/analisi-intelligence*).

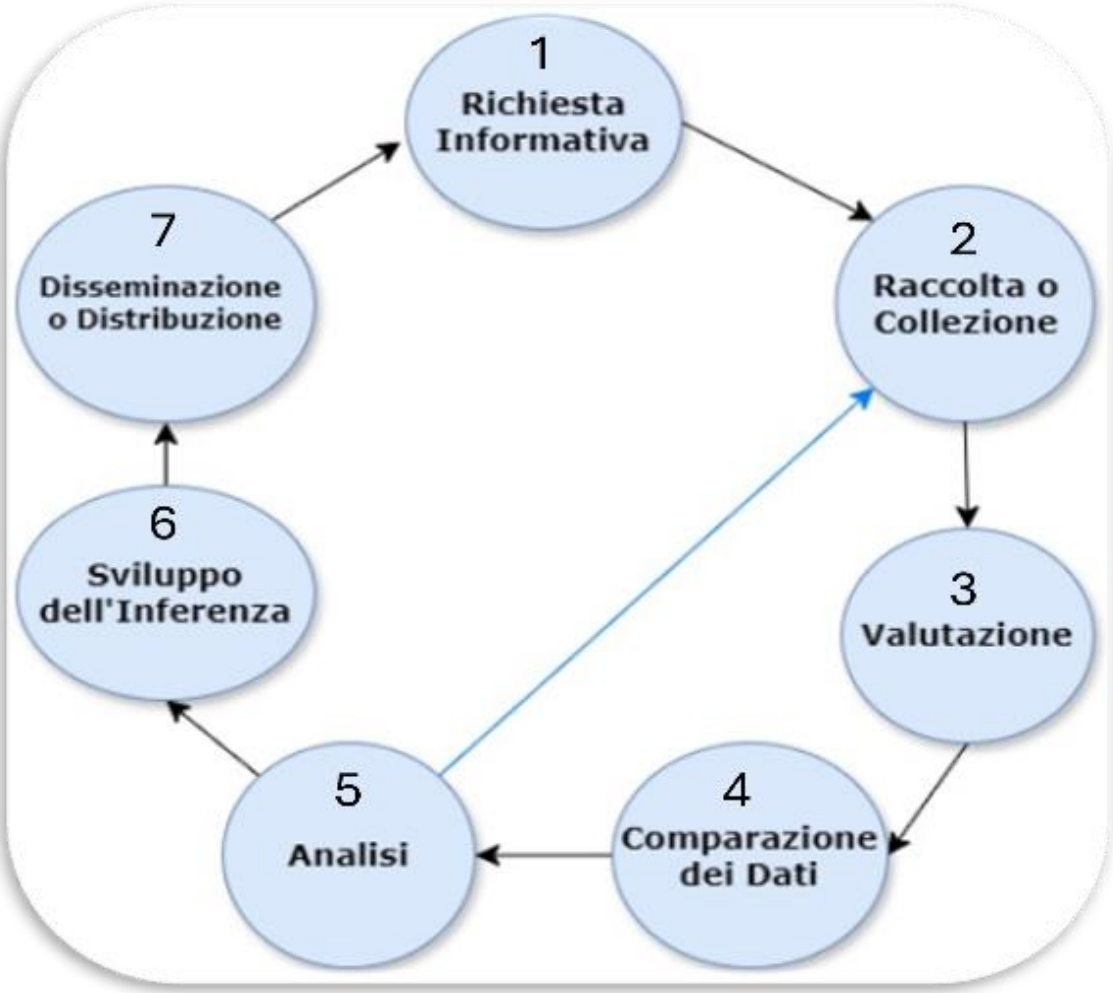
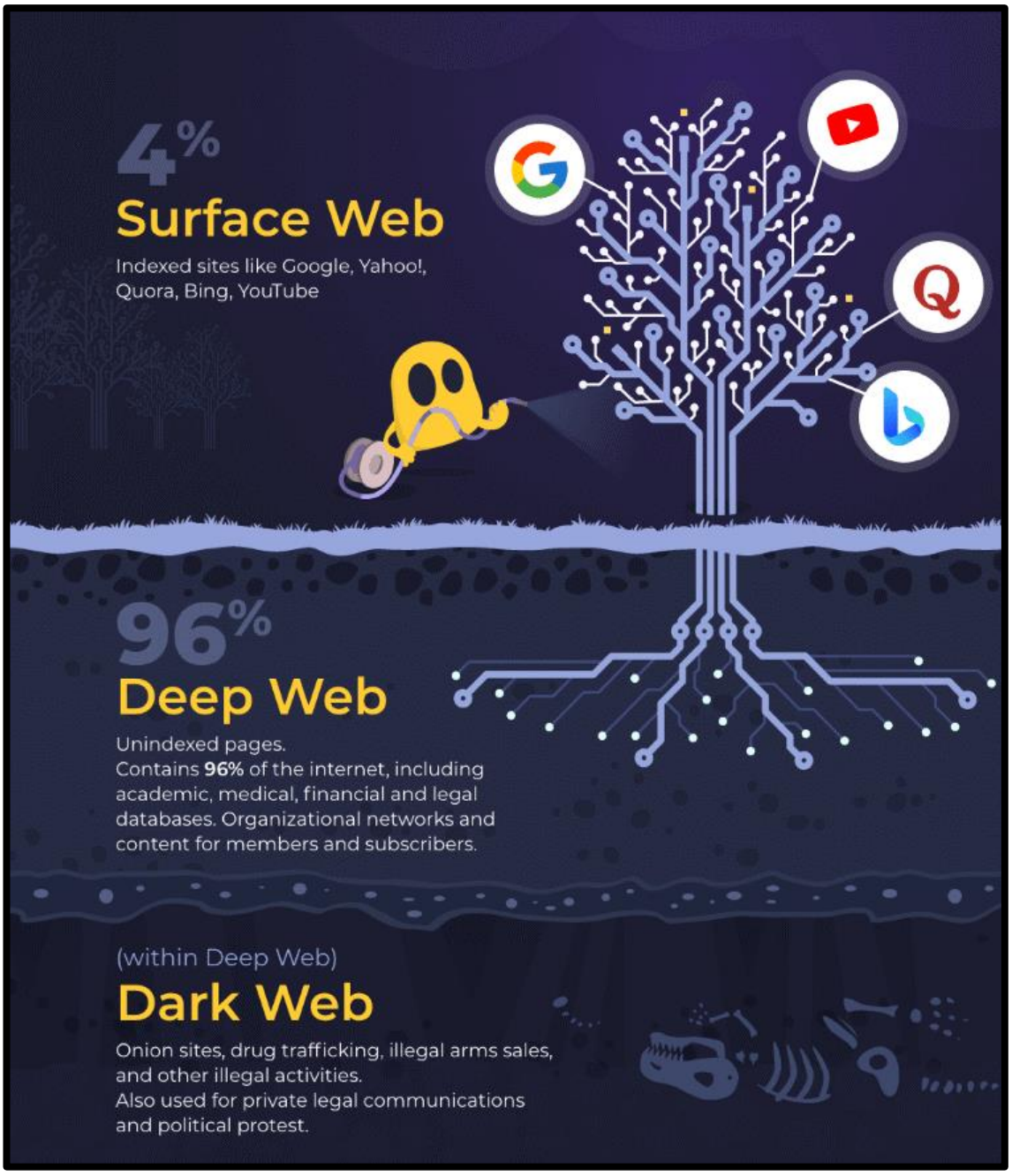


Figura 9:- Ciclo dell'Intelligence

4. DOVE STIAMO OPERANDO NEL CLEARWEB O DEEPWEB?

Prima di iniziare la nostra attività di ricerca o raccolta informativa è bene fare una premessa su quali sono i campi in cui un analista OSINT opera, ovvero andare a definire cosa si intende per ClearWEB, DeepWEB e DarkWEB.

Il **ClearWEB** o **SurfaceWEB,** è l'arte di internet che conosciamo tutti ed è la parte di internet a cui tutti noi accediamo quotidianamente. Comprende siti web e risorse indicizzate dai motori di ricerca come Google, Yandex o Bing. Pensate a tutto ciò che potete trovare attraverso una semplice ricerca Google; questo rappresenta solo una frazione dell'intero universo di internet, più precisamente circa il 4-10% del totale.



Passiamo ora al **DeepWEB,** che è sostanzialmente tutto ciò che non è indicizzato dai motori di ricerca standard. Questo include una vasta gamma di contenuti, da banche dati accademiche a documenti governativi, registri ospedalieri, e persino le vostre e-mail personali. Importante è sottolineare che il DeepWEB non è per natura oscuro o illegale; è semplicemente non accessibile tramite i normali motori di ricerca per motivi di *privacy* e sicurezza.

Dentro il DeepWEB, troviamo la **Darknet** (detta anche DarkWEB), che rappresenta una piccola porzione del DeepWEB. La Darknet è intenzionalmente nascosta e accessibile solo tramite software specializzati, il più noto dei quali è TOR, acronimo di *The Onion Router*. La caratteristica principale di TOR è la sua capacità di anonimizzare le connessioni degli utenti, mascherando l'identità e la posizione di chi naviga e di chi ospita i servizi. Uno dei più noti software che incontreremo più avanti per accedere alla rete TOR è **TOR Browser**, ma anche **Brave** che ha un modulo al suo interno che permette la navigazione.

Uno dei miti da sfatare è che accedere alla rete TOR, sia illegale. In realtà è uno strumento che viene usato principalmente per la libertà digitale, specie in quei paesi dove non vi è libertà di espressione. Di fatti utilizzando questa rete, attivisti e giornalisti riescono a comunicare in modo sicuro ed accedere liberamente a diverse fonti. Tuttavia, non è da ignorare la presenza di molteplici attività criminali come il traffico di droga, vendita di armi, vendita di dati personali, vendita di documenti falsi, produzione di filmati pedopornografici etc.

5. USO ED INSTALLAZIONE DI UNA VPN

Iniziamo col dire cos'è una VPN, ovvero una Virtual Private Network. È un software che crea connessioni sicure e crittografate tra il proprio dispositivo (PC o Smartphone, etc.) e un server gestito dal provider della VPN (es. NordVPN). Questo tunnel crittografato ci permette di garantire che i dati trasmessi siano sicuri e privati.

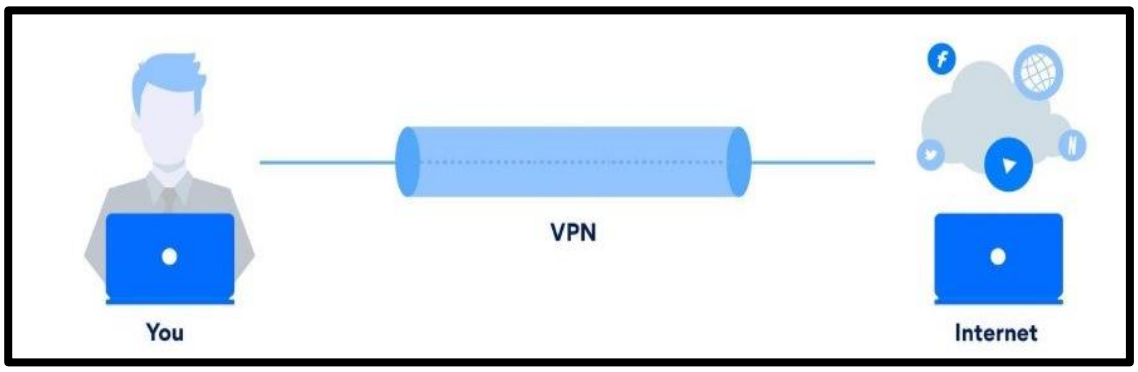


Figura 10:- Esempio di Connessione VPN

Ciò è utile per:

- proteggere i propri dati personali durante la navigazione;
- arginare eventuali censure e restrizioni nell'area geografica dove ci troviamo (esempio giornalisti investigativi che operano in paesi totalitari);
- ulteriore sicurezza quando ci si connette in reti pubbliche.

Detto questo, è facilmente intuibile quali sono le ragioni per cui la VPN è uno degli elementi fondamentali durante il lavoro di analisi OSINT. In particolare:

- *protezione dell'identità*: grazie al fatto che nasconde l'indirizzo IP dell'operatore reale, riesce a proteggere la sua identità durante tutta la raccolta delle informazioni;
- *migliorare la capacità di ricerca delle informazioni*: collegandosi ad un server estero, possiamo visualizzare ed acquisire informazioni da un server locale (per esempio, raccolta di informazioni ad un utente in Africa, scegliamo il server che si trova nello stesso Paese del target o di quello adiacente).

Figura 11:- Esempio dei Server di un Software di VPN

6. PASSWORD MANAGER

L'uso di un gestore di password (*Password Manager*) è una pratica che può aiutare gli utenti a gestire in modo sicuro ed efficiente le loro credenziali di accesso. Di fatti quando si creano molti avatar a cui si associano diversi profili social e servizi è impossibile a volte ricordarsi tutte le password. Per questo è importante dotarsi di un software simile ed una multipiattaforma che possiamo usare per avere sempre con noi in pochi attimi tutti gli accessi ai servizi ed agli avatar di cui disponiamo.

I gestori di password sono strumenti che memorizzano e organizzano password ed altri dati sensibili, crittografandoli in un "cassaforte" digitale protetta da una master password unica.

7. CREAZIONE DI UNA WORKSTATION

Definito in quale ambiente stiamo operando è importante creare il nostro ambiente di lavoro.

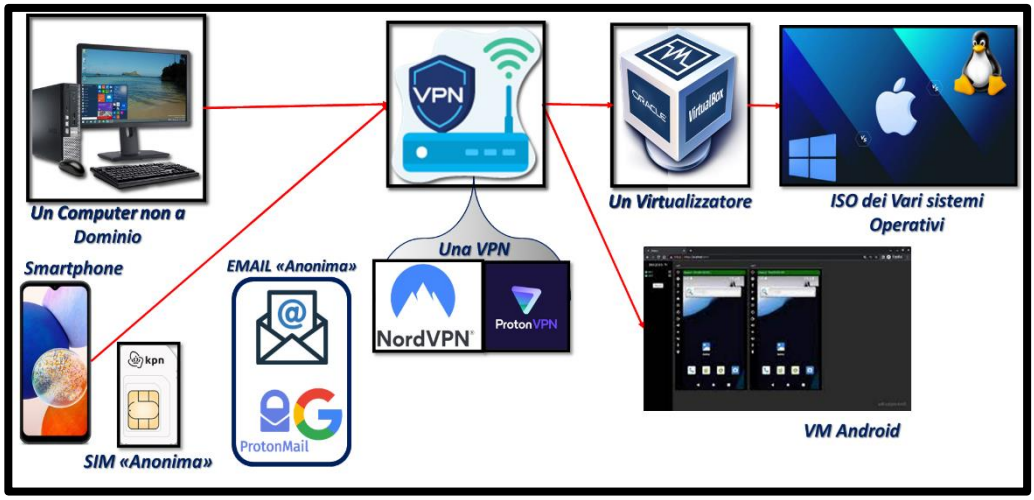
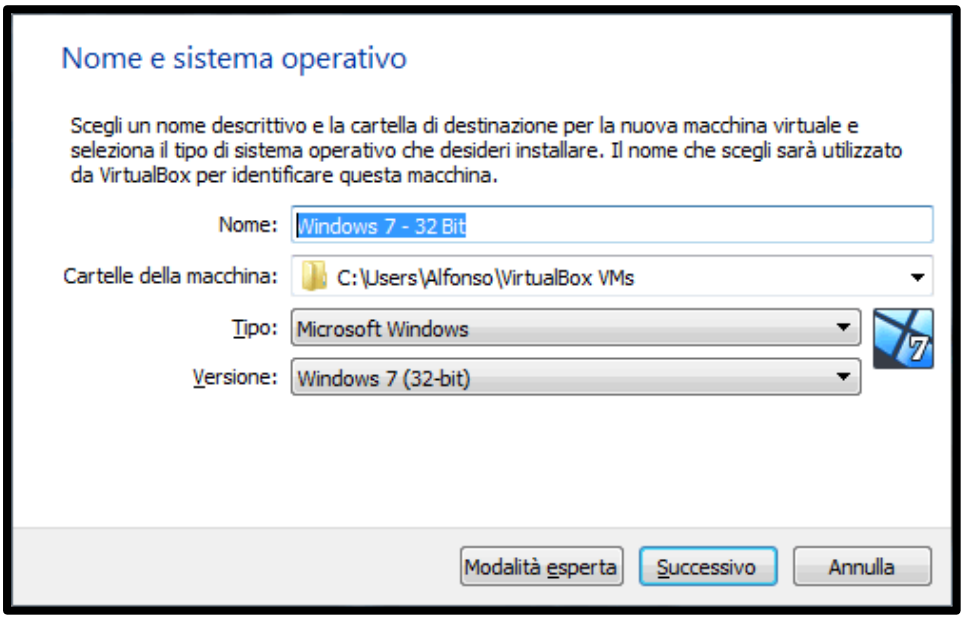


Figura 12:- Creazione di una Workstation per OSINT

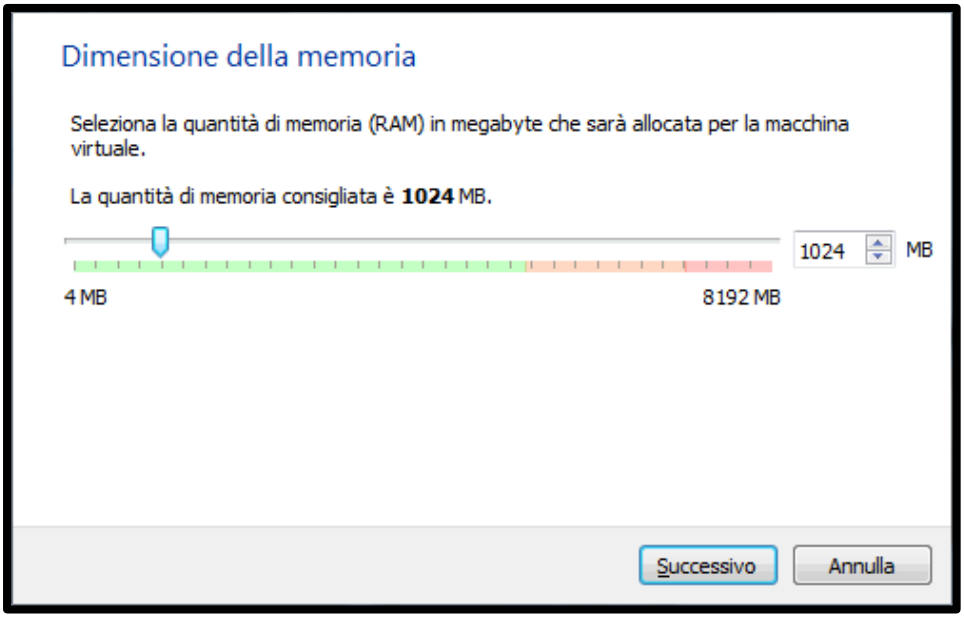
Creare una Workstation specificamente configurata per l'attività di OSINT, richiede attenzione a diversi aspetti tecnologici e di sicurezza. Iniziamo con un computer senza dominio istituzionale ed infine installiamo un software per la virtualizzazione come VMware o VirtualBox.

Di seguito indicheremo i passaggi per la creazione della nostra macchina Virtuale con il software VirtualBox. Dopo aver scaricato e installato tramite il sito *https://www.virtualbox.org/wiki/Downloads* la versione più aggiornata di VirtualBox e l'Extension Pack, procediamo all'installazione della nostra macchina virtuale.

1. Cliccare su Nuova.

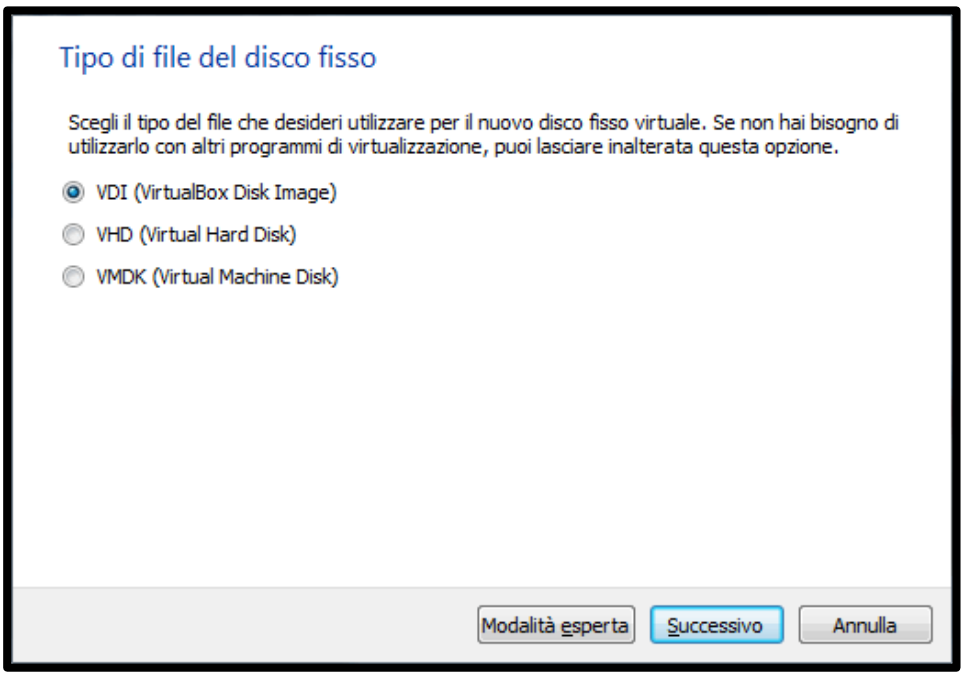


2. Inserire un nome del sistema operativo che vogliamo configurare. Scegliamo in quale cartella inserire tutti i file che comporranno la nostra VM (Virtual Machine), scegliere che tipo di VM si vuole inizializzare (Windows. Linux o Mac) e la versione.

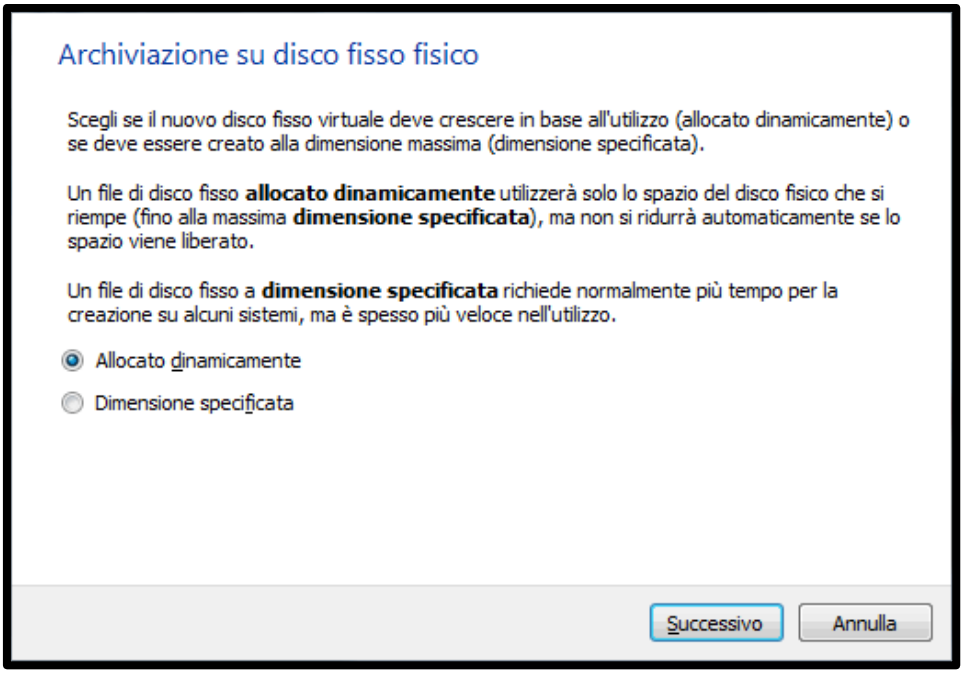


3. Scegliere la quantità di RAM necessaria per lavorare sulla nostra VM.

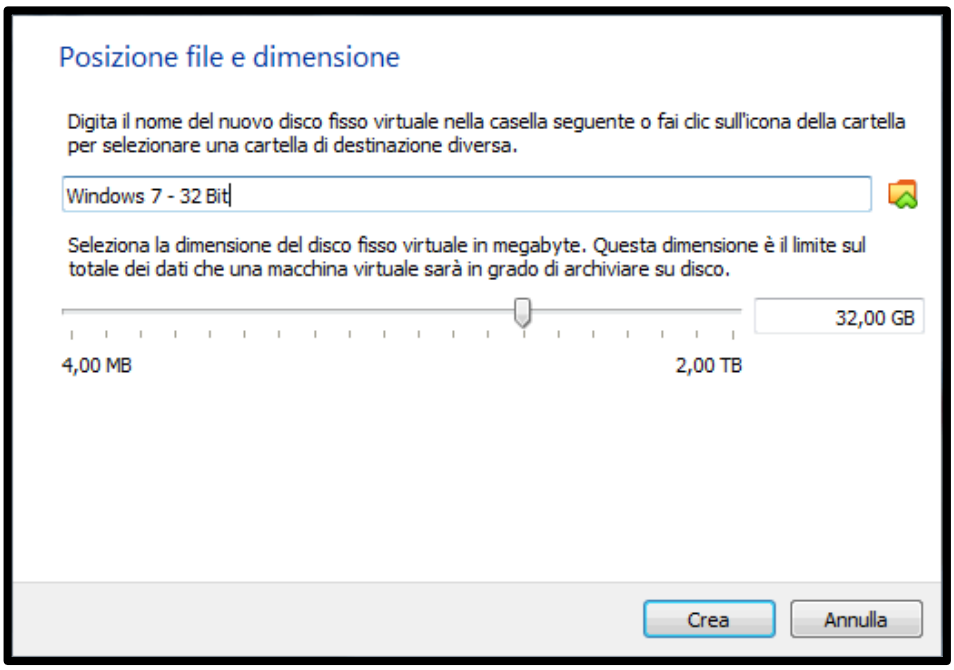
4. Possiamo inserire un disco virtuale già esistente, oppure crearne uno nuovo.



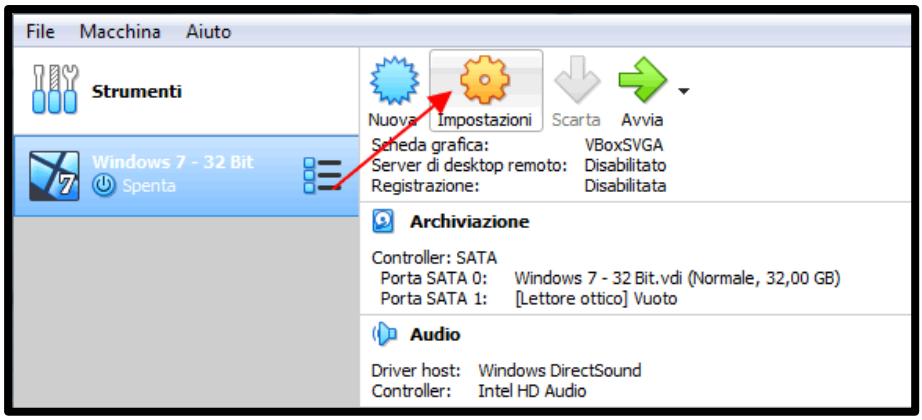
5. Scegliere l'estensione del disco che vogliamo creare. Questo può essere importante se poi vogliamo utilizzare la nostra VM su un'altra piattaforma o un altro computer che ha installato un software di virtualizzazione come VMware o Hyper-V.



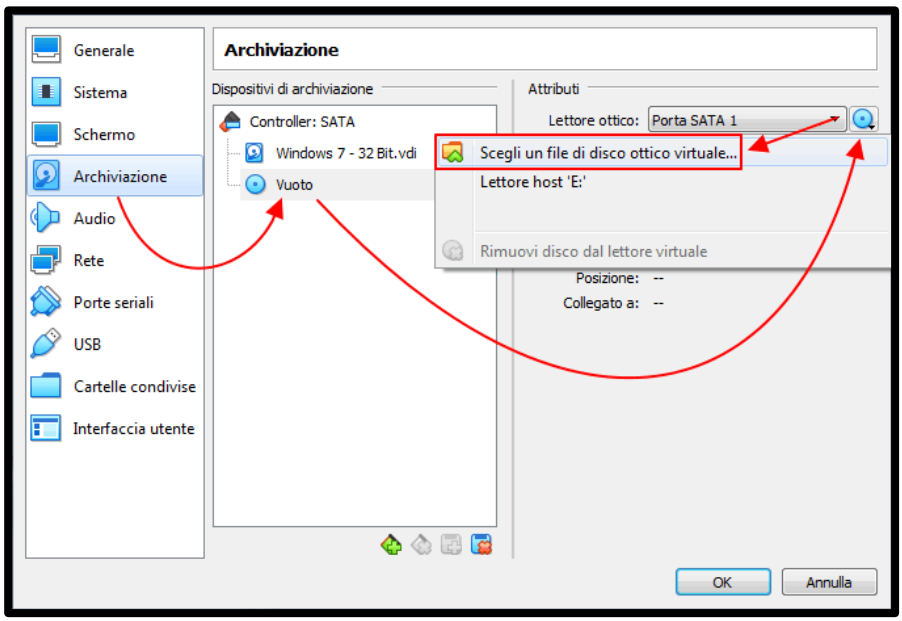
6. Scegliere la tipologia di archiviazione sul disco fisso, se dinamico o con archiviazione massima.

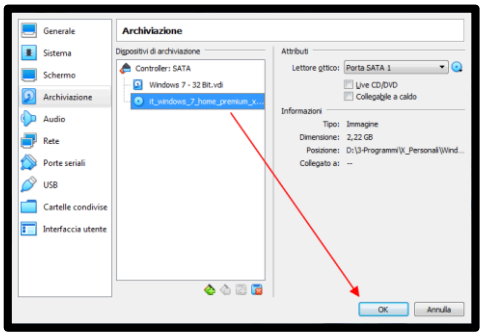


7. Scegliere dove archiviare il disco e la sua dimensione e premere su Crea.

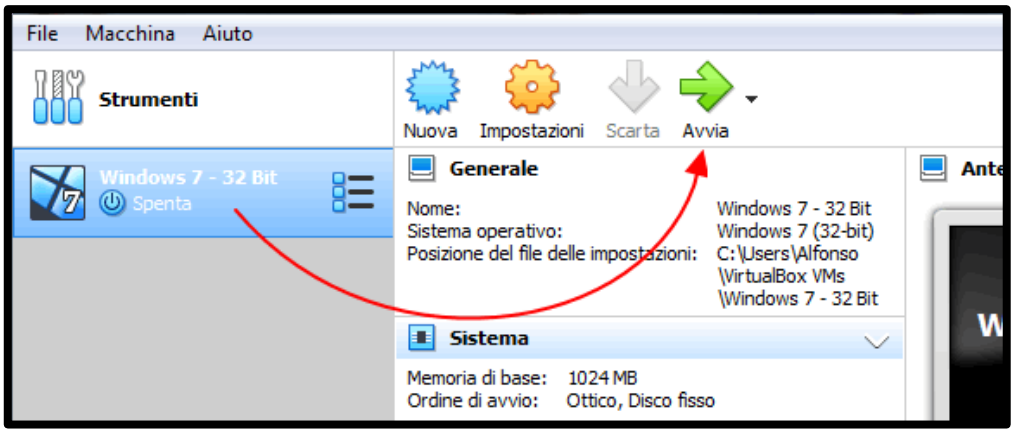


8. Una volta creata la nostra macchina virtuale, dobbiamo inserire il nostro sistema operativo all'interno. Una volta selezionata la nostra macchina virtuale, andiamo su Impostazioni.





9. Andiamo su “Archiviazione”, clicchiamo sul disco vuoto e poi clicchiamo “scegli un file di disco ottico virtuale…”, successivamente andiamo nella cartella che contiene la nostra .iso e la carichiamo e infine premiamo “ok”.



10. Adesso possiamo avviare la nostra macchina virtuale o con un doppio click oppure premendo il pulsante Avvia.

8. ISO E DISTRO LINUX WINDOWS E MAC

Una volta capito come creare una macchina virtuale, bisogna capire che tipo di immagine vogliamo utilizzare per la nostra attività.

Esistono diversi tipi di immagini a seconda della modalità di lavoro e dell'impostazione della nostra VM. Iniziamo dalle più comuni che sono:

- **Kali Linux** - *https://www.kali.org/get-kali/*
- **Tsurugi Linux (v. Lab)** - *https://tsurugi-linux.org/downloads.php*
- **Parrot Security OS** - *https://www.parrotsec.org/download/*
- **CSI Linux** - *https://csilinux.com*
- **Tails** - *https://tails.net/install/index.it.html*

Figura 13:- Virtual Machine Linux

Successivamente esistono delle VM già configurate con tutti i tools che ci servono per la nostra attività di OSINT, come:

- **AnuBitux** - *https://anubitux.org/download-anubitux/*
- **OSINTko** - *https://github.com/LinaYorda/OSINTko*
- **SIFT Workstation** - *https://www.sans.org/tools/sift-workstation/*

9. BROWSER E MOTORI DI RICERCA

L'uso di browser dedicati o configurati specificamente per l'attività di Open Source Intelligence (OSINT) è fondamentale per garantire sicurezza, anonimato ed efficacia durante la raccolta di informazioni e non solo. Come vedremo alcuni di questi software sono nati proprio per garantire il massimo della *privacy* all'utente, altri invece possono essere configurati in maniera apposita. Di seguito andremo a vedere tre dei principali browser che sono utilizzati per la navigazione su internet.

9.1. TOR BROWSER

Tor Browser è basato su Mozilla Firefox ed è progettato per rendere anonimo il traffico degli utenti utilizzando la rete Tor che nei capitoli precedenti abbiamo già affrontato. Questo processo, noto come routing "onion", cripta i dati più volte e li passa attraverso diversi nodi, rimuovendo ad ogni passaggio uno strato di crittografia. Questo percorso rende estremamente difficile tracciare l'origine del traffico, garantendo l'anonimato dell'utente. Questo browser è particolarmente utile per gli analisti OSINT che necessitano di nascondere il loro indirizzo IP e la loro ubicazione geografica per accedere ad informazioni protette da restrizioni geografiche o per salvaguardare la loro identità.

Tra le sue caratteristiche abbiamo quindi:

- **Anonimato:** Tor Browser maschera l'indirizzo IP dell'utente, rendendo quasi impossibile per i siti web, gli inserzionisti e gli eventuali osservatori esterni individuare la vera origine del traffico;
- **Accesso a siti web. onion:** la rete Tor ospita siti web speciali con estensione ".onion", che non sono accessibili tramite browser tradizionali. Questi siti offrono ulteriori livelli di *privacy* e anonimato;
- **Protezione contro il tracciamento**: Tor Browser è configurato per bloccare i tracker e i tentativi di *fingerprinting* del browser, che cercano di identificare gli utenti tramite le configurazioni del loro dispositivo;
- **Sicurezza predefinita:** il browser offre diversi livelli di sicurezza che gli utenti possono regolare a seconda delle loro necessità. Queste impostazioni influenzano elementi come l'esecuzione di JavaScript, i font e altri componenti che possono essere utilizzati per tracciare gli utenti.

Installazione e Settaggi *privacy*

Essendo multipiattaforma, TOR lo possiamo installare tramite:

- link - *https://www.torproject.org/*
- riga di comando attraverso il terminale di Linux:

- *Sudo add-apt repository-y ppa:micahflee/ppa*
- *Sudo apt-y update*
- *Sudo apt install-y torbrowser-laucher*

- store di Google Play e Apple App-Store.

9.2. MOZILLA FIREFOX

Firefox è altamente personalizzabile e può essere configurato con varie estensioni e impostazioni per migliorare la sicurezza e la *privacy*. È uno dei browser web più popolari e rispettati, noto per la sua flessibilità, per le sue robuste funzionalità di *privacy* e per la sua aperta filosofia di sviluppo. È creato e distribuito da *Mozilla Foundation*, un'organizzazione no-profit dedicata alla promozione di un internet aperto e accessibile.

Tra i suoi pregi abbiamo:

- **la modalità di navigazione privata**: impedisce il salvataggio della cronologia di navigazione e dei cookie;
- **protezione migliorata da tracciamento:** Firefox blocca automaticamente molti tracker di terze parti, incluso il tracciamento dei contenuti in incognito e i cookie cross-site;
- **modalità di navigazione privata:** simile ad altri browser, la modalità privata di Firefox non salva la cronologia di navigazione o i cookie;
- **protezioni contro il fingerprinting:** Firefox include protezioni contro tecniche di fingerprinting avanzate che cercano di identificare gli utenti basandosi sulle configurazioni dei loro dispositivi.

Installazione e Settaggi *privacy*

Essendo anche lui multipiattaforma, possiamo installare il browser tramite:

- sito Internet: *https://www.mozilla.org/en-US/firefox/new/*
- riga comando del terminale di Linux:
  - Sudo snap install firefox
- store di Google Play e Apple App-Store.

Inoltre, esistono due metodi, uno base ed uno avanzato per aumentare la sicurezza e la *privacy* del browser.

- **Configurazione Base:** attraverso la voce Menu - Opzioni - *Privacy* e Sicurezza, possiamo:
    - attivare “Cancella cookie e dati dei siti quando Firefox viene chiuso”;
    - attivare “Avvisami quando i siti web tentano di installare componenti aggiuntivi”.
- **Configurazione Avanzata**
    - inserire **about:config** nella barra degli indirizzi e procedi a “mostra tutto”.
    - procedere con le seguenti configurazioni:

imposta su **Falso**:	imposta su **Vero**:
Feo.enabled, *Browser.safebrowsing.* *Phishing.enabled,* *Browser.safebrowsing.malware.enabled,* *Media.navigator.enabled,* *dom.battery.enabled,* *Extensions.pocket.enabled,* *Media.peerconnection.enabled,* *Media.peerconnection.use,* *Document.iceservers,* *Media.peerconnection.video.enabled.*	*Media.peerconnection.turn.disable.*

9.3. BRAVE

Il browser Brave è diventato popolare per il suo focus sulla *privacy* e sicurezza online. È costruito sullo stesso motore di *Chromium*[2], che alimenta anche Google Chrome, ma si distingue per alcune caratteristiche chiave orientate alla *privacy*.

Tra le sue principali caratteristiche abbiamo:

- **blocco degli annunci e dei tracker:** Brave blocca automaticamente annunci e tracker durante la navigazione. Questo non solo velocizza la navigazione ma protegge anche gli utenti dal tracciamento *cross-site*. Questo significa che durante la navigazione si possono visualizzare ed analizzare siti senza modificare significativamente il proprio profilo digitale o lasciare tracce.
- **protezione avanzata contro il fingerprinting:** il fingerprinting è una tecnica usata per identificare univocamente i visitatori di un sito web attraverso la combinazione di diverse informazioni del loro dispositivo. Brave offre protezioni avanzate contro il fingerprinting, in modo da minimizzare la propria visibilità.
- **Tor integrato:** Brave include la possibilità di aprire una scheda privata con Tor, che offre un ulteriore livello di *privacy* nascondendo l'indirizzo IP e criptando il traffico web attraverso la rete Tor.
- **HTTPS Everywhere:** Brave integra "*HTTPS Everywhere*", che forza la connessione a siti web tramite HTTPS quando disponibile, garantendo una connessione criptata e più sicura.
- **wallet di criptovalute integrato:** inoltre offre un *wallet* integrato per criptovalute, che potrebbe essere utile per chi si occupa di investigazioni relative a transazioni blockchain o criptovalute.

Installazione e Settaggi *privacy*

L'installazione del Browser Brave può avvenire:

- Sito
  - *https://brave.com*

[2] Chromium è un progetto di browser Web gratuito e open source, sviluppato e gestito principalmente da Google. Si tratta di una codebase ampiamente utilizzata, che fornisce la stragrande maggioranza del codice per Google Chrome e molti altri browser, tra cui Microsoft Edge, Samsung Internet e Opera. Il codice viene utilizzato anche da diversi framework di app.

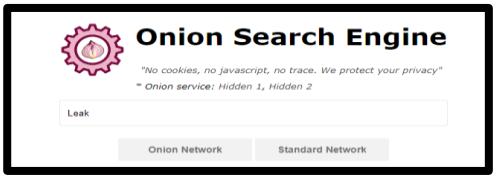
- Riga di comando linux
    - *sudo apt install curl*
    - *sudo curl -fsSLo /usr/share/keyrings/brave-browser-archive-keyring.gpg*
    - *https://brave-browser-apt-release.s3.brave.com/brave-browser-archive-keyring.gpg*
    - *echo "deb [signed-by=/usr/share/keyrings/brave-browser-archive keyring.gpg] https://brave-browser-apt-release.s3.brave.com/ stable main"|sudo tee /etc/apt/sources.list.d/brave-browser-release.list*
    - *sudo apt update*
    - *sudo apt install brave-browser*

9.4. MOTORI DI RICERCA

Sebbene Google sia un motore di ricerca potentissimo ed efficiente, non è l'unica opzione che abbiamo, di fatti esistono ulteriori motori di ricerca che ci permettono di esplorare vari dati che Google non ci fa vedere per varie ragioni e che ci possono permettere di stringere il campo su quelle che sono le nostre ricerche.

Tra questi motori di ricerca abbiamo:

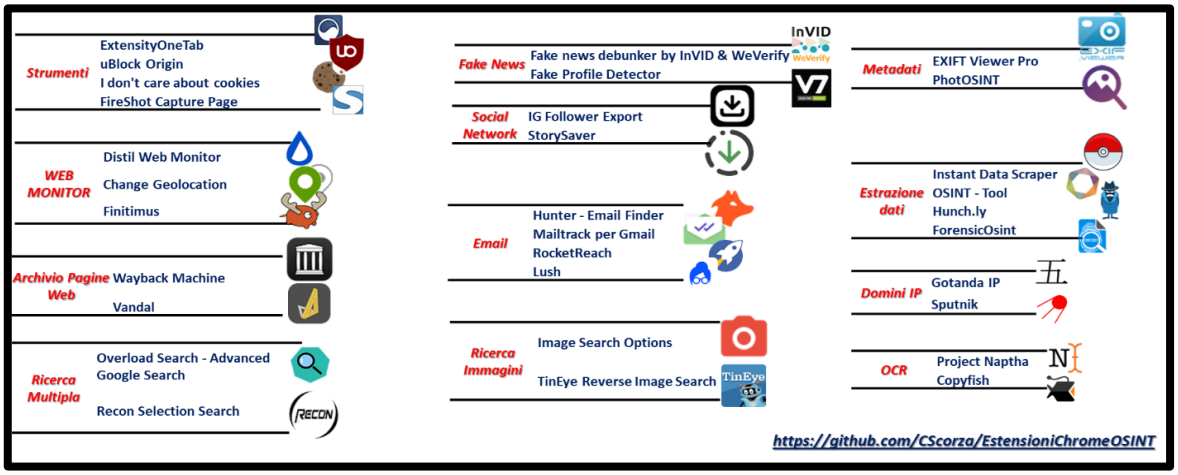
- ***DuckDuckGo*** **(***https://duckduckgo.com/***)**, *ottimo per la privacy dell'utente, ma anche perché utilizza un operatore di ricerca specifico per Paese. Inoltre permette di effettuare ricerche su siti .onion*
- ***Yandex*** ***(****https://yandex.com****)*** *orientato per le ricerche in Russia ed Europa orientale, è molto efficiente per il Reverse Image (ricerca per immagini) e la traduzione di testi presenti nelle immagini.*
- ***Baidu*** ***(****https://baidu.com****)*** *è uno dei motori di ricerca più usato nell'Asia Orientale (in particolare in Cina), di fatti è un motore di ricerca che indicizza molti siti presenti in quell'aerea geografica.*



- ***Onionengine*** ***(****https://onionengine.com****)*** *è uno dei tanti motori di ricerca per siti .onion, quindi tutti quei servizi che stanno sulla rete Tor.*

9.4.1. ESTENSIONI PER IL BROWSER

Oltre al Browser e al motore di ricerca, esistono ulteriori strumenti che possono essere utilizzati per la nostra raccolta di dati. Questi strumenti prendono il nome di "Estensioni – *add-ons*" e di norma sono presenti in tutti i browser più diffusi come FireFox, Brave e Google Chrome. Essi si integrano al software per la navigazione ad internet e ci aiutano a raccogliere e analizzare le pagine web che stiamo esplorando e altro ancora. Ovviamente è estremamente consigliato, tranne in casi eccezionali il download e l'installazione di questi strumenti, solo dalla fonte ufficiale.



Per l'attività di OSINT ve ne sono di molti tra famosi e meno famosi. Qui di seguito ne riportiamo alcuni che possono essere d'aiuto.

Strumenti per l'anonimato e controllo privacy	***UBlock Origin***	***NoScript***
	Ghostery - Ad Blocker per la Privacy	***I don't care about cookies***
Cattura Schermo - Scraping	***ForensicOsint***	***Nimbus Screenshot***
	Go Full Page	***FireShot Capture Page***
	Hunch.ly	***OSINT - Tool***
	Tinking - Scrapping Tool	***Instant Data Scraper***
Web Monitor	***Change Geolocation***	***Finitimus***
Metadati	***EXIFT Viewer Pro***	***PhotOSINT***
Deepfake	***Fake news debunker***	***Fake Profile Detector***
Multi Ricerca	***Overload Search***	***Recon***
	Selection Searc	
Archivio Pagineweb	**Wayback Machine**	***Webrecorder ArchiveWeb.page***
	Vandal	

Ricerca Immagini	***Image Search Options***	**RevEye Reverse Image Search**
	TinEye Reverse Image Search	**Download All Image**
Analisi E- Mail	***Hunter - Email Finder Extension***	**Mailtrack per Gmail: Email tracking**
Ricerca E-Mail sui Social	*RocketReach*	***SignalHire***
Social Network	***IG Follower Export too***	**Story Saver**
	Treeverse (Twitter)	
Analisi Dei Domini	***Gotanda***	***IP Address and Domain Information***
	Sputnik	

Figura 14:- Estensioni utili per il Browser

10. SOCMINT - SOCIAL MEDIA INTELLIGENCE

La Social Media Intelligence è un ramo dell'intelligence che si concentra sulla raccolta e analisi delle informazioni disponibili sui social media per diversi scopi, tra cui sicuramente raccolta d'informazioni di carattere d'intelligence o per informazioni strategiche.

Questo ramo dell'OSINT sfrutta i dati lasciati dagli utenti, i loro comportamenti online e le varie interazioni tra i vari utenti sui social network come Facebook, Instagram, Twitter, Linkedin etc.

Le principali attività del SOCMINT sono:

- **Analisi del contenuto**: che include l'analisi dei post, dei commenti, delle immagini e dei video pubblicati dagli utenti sui social media. Questo permette di comprendere le opinioni, i sentimenti e le tendenze che possono emergere dalla quantità di dati generati dagli utenti.
- **Analisi della rete:** l'analista in questa fase, esplora le reti sociali per identificare le connessioni tra gli utenti, come le reti di amicizie, le influenze reciproche etc.

- **Geolocalizzazione:** molti post nei vari social media, includono dati di geolocalizzazione, che possono essere utilizzati per determinare dove gli utenti si sono trovati al momento della pubblicazione.

Ovviamente tutti questi dati hanno bisogno di un ulteriore verifica ed analisi, in quanto sono dati inseriti dall'utente e quindi facilmente falsificabili.

10.1. CREAZIONE DI UN AVATAR (SOCKPUPPET)

Uno dei pilastri fondamentali per ogni analista OSINT, è quello di creare diversi avatar o sockpuppet (ovvero entità fittizie), usati per la raccolta di informazioni senza rilevare quindi la vera identità dell'operatore. L'uso di avatar è fondamentale per accedere a diverse informazioni nei vari ambienti online. Pensiamo a forum presenti sulla Darknet o determinati social network che fanno notare la visualizzazione del proprio profilo all'utente che si sta analizzando. Inoltre, è fondamentale anche la sua creazione al fine di renderlo quanto più credibile possibile nell'ambiente che stiamo esplorando. Per questo di seguito vedremo i vari passaggi che ci possono aiutare nella creazione della nostra identità, dalla creazione di una biografia credibile, alla scelta dell'immagine del profilo, all'uso di una SIM non intestata alla scelta di un'e-mail sicura.

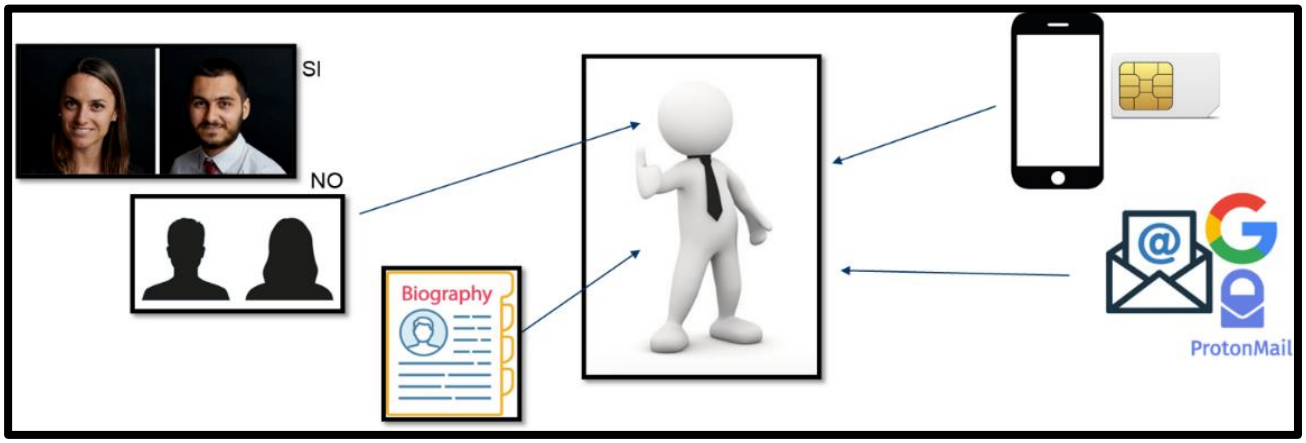


Figura 15:- Elementi per la creazione di un AVATAR

10.2. BIOGRAFIA

La creazione di una biografia convincente per un avatar richiede attenzione ai dettagli e la comprensione del contesto in cui l'avatar dovrà operare e quindi il suo impiego.

Quindi una delle domande che bisogna farsi durante la creazione della biografia è:

- Qual è l'obiettivo dell'operazione? (raccolta d'informazioni o monitoraggi di un target specifico);
- In quale ambiente andrà ad operare? (Dark WEB, Social Network e il contenuto in cui si muoverà);
- In quale contesto? (terrorismo religioso, politico, gruppi hacker, pedopornografia etc.).

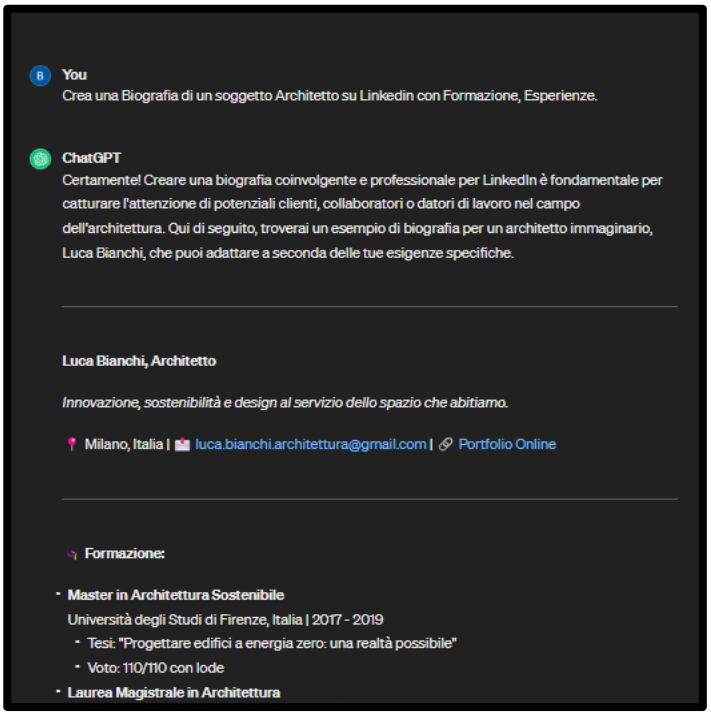


Figura 16:- Creazione di una Biografia con Chat GPT

Per questo bisogna sviluppare un "*background*" personale che includa, non solo il nome e cognome, ma anche un'età anagrafica coerente, luogo di residenza/nascita, formazione, carriera ed occupazione oltre ad hobby e vari interessi. Va da sé che la scelta d'inserire queste informazioni varia sempre in base al contesto in cui vogliamo operare. Infatti, ci saranno dei contesti dove le informazioni da inserire sono minime in modo da non destare particolare sospetto, oppure contesti più ricchi in modo da non correre rischi se ci fosse un riscontro dal nostro target o addirittura dal social stesso che potrebbe bannarci per operazioni sospette.

Tra i vari strumenti che possiamo usare ci sono sicuramente:

- ChatGPT di OpenAI
- Gemini
- Fake Name Generator - *fakenamegenerator.com*
- *Randus.org*

10.3. IMMAGINE DEL PROFILO

Dopo aver creato la biografia del nostro avatar, dobbiamo trovare un'immagine profilo da inserire nel social. Per questo è importante considerare diversi fattori, tra cui la credibilità dell'immagine e che sia appropriata al contesto in cui stiamo operando. Di fatti è importante non usare immagini di persone reali e magari optare per immagini generiche come quelle di loghi o paesaggi, quadri d'arte o simboli. Ma molte volte è necessario avere delle immagini di persone, per esempio dalle politiche del gruppo social dove ci stiamo inserendo oppure dalle politiche del social network. Per questo problema possiamo ricorrere a diverse soluzioni come:

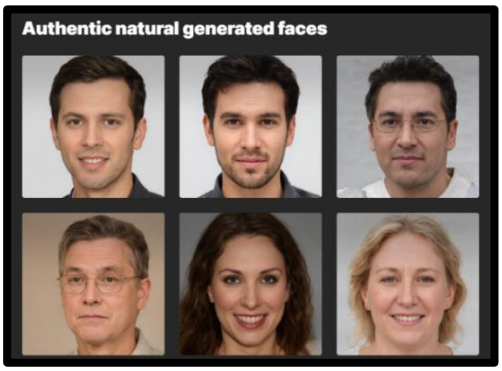


Figura 17:- Authentic natural Generated.photos/faces

- *Thispersondoesnotexist.com*
- *Randus.com*
- *Generated.photos/faces*

Questi strumenti come altri permettono di creare immagine di volti falsi creati grazie alle reti generative (GANs) e ci permettono di modificare a nostro piacimento il volto in modo da poterlo inserire sia nel contesto della biografia che abbiamo creato (pensiamo all'età, etnia etc.) sia nel contesto dove l'avatar andrà ad operare.

10.4. E-MAIL

Dopo aver creato la biografia e l'avatar, passiamo alla creazione di strumenti per l'iscrizione ai social network, come e-mail e numero di telefono. Tra gli strumenti che andremo a vedere, ci sono:

- ProtonMail - *proton.me/mail*
- Simplelogin - *simplelogin.io*

Partendo dall'email il servizio più usato per la sua affidabilità e sicurezza è sicuramente **ProtonMail**. Questo perché utilizza la criptografia end-to-end, in modo che solo l'utente e il destinatario possono accedere al contenuto delle e-mail inviate. Inoltre non

conserva file di log e permette di creare diversi alias di e-mail legate a quella madre, in modo da gestire diverse entità.

Oltre a ProtonMail sicuramente la posta elettronica di Google (Gmail) può esserci utile per accreditarci ad un social network. Questo perché le politiche d'iscrizione al social, non permettono l'uso di ProtonMail.

Figura 18:- Pronton Mail

Un altro strumento è **Simple Login**.

Questo strumento permette di generare di versi alias di e-mail che inoltrano i messaggi alla loro casella di posta elettronica principale. Questi alias possono essere personalizzati, disattivati o eliminati in qualsiasi momento e questo ci permette un controllo completo e flessibile a tutte le nostre entità.

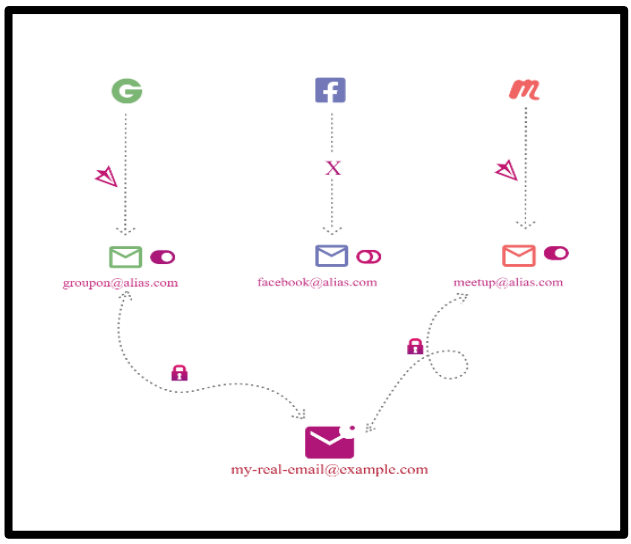


Figura 19:- Simple Login.

10.5. NUMERO DI TELEFONO

In molti casi durante la registrazione all'interno di un social o la creazione di un'e-mail è richiesto un numero di telefono per autenticare il profilo. Ovviamente per diversi motivi non è consigliato l'uso del proprio numero personale. Per questo esistono diversi metodi per inserire dei numeri di telefono temporanei che non siano direttamente riconducibili all'analista.

Questi servizi sono:

- **Servizi di ricezione SMS**
    - *https://onlinesim.io/*
    - *https://receivesms.co/available-countries/*
    - *https://getfreesmsnumber.com/*
    - *https://anonymsms.com/temporary-phone-number/*

- *https://quackr.io/*
- *https://sms-activate.org/en*
- *https://getsms.online/en/*

- **Servizi eSIM**
  - *https://www.airalo.com/it*
  - *https://voice.google.com/u/0/about*
- **SIM fisiche estere**

10.6. USO DEI SOCIAL NETWORK PER IL SOCIMINT

Una delle principali fonti di ricerca d'informazioni sono i *Social Network.* Esso infatti rappresenta un potente strumento per raccogliere, analizzare e monitorare informazioni relative a persone, organizzazioni ed eventi d'interesse.

Il primo passo, una volta identificati i social network frequentati dal nostro target, consiste nel registrare un profilo fittizio (sockpuppet/avatar). Questo ci permette, se possibile, di accedere alle pagine profilo e raccogliere i dati che altrimenti non sarebbero visibili.

Di seguito vediamo quali sono i social più diffusi e quali tools usare per la nostra attività di OSINT.

10.6.1. FACEBOOK

Facebook è uno dei più famosi social di META e grazie anche alla vasta diffusione che ha avuto negli anni, è per l'analista una fonte enorme per la quantità d'informazioni e dati che si possono ricavare. Infatti, tramite i profili dei nostri target è possibile ricavare molte informazioni come:

- ***l'ID:*** *ovvero un identificatore univoco assegnato a ciascun account utente;*
- ***Dati Anagrafici:*** *nome e cognome, data e luogo di nascita e posto dove si vive;*
- ***Contatti:*** *numeri di telefono ed e-mail;*
- ***Reti di amicizie e parentele:*** *è possibile identificare quali sono gli utenti più attivi ed eventuali legami di parentele;*
- ***Hobby e informazioni personali:*** *attraverso i post e le informazioni inserite da ogni singolo utente è possibile ricavare tutta una serie d'interessi;*
- ***Geolocalizzazione delle immagini e video:*** *con la geolocalizzazione che l'utente inserisce nelle immagini ma anche dal contesto che rappresenta l'immagine stessa è possibile sapere in quale luogo è stata scattata;*
- ***I "Tag" delle foto****: con i Tag possiamo anche sapere i nominativi delle persone "taggate" nelle foto e video.*

TOOLS FACEBOOK

Dei tools usati per l'analisi dei profili Facebook sono:

- **FuckFacebook**
  https://4wbwa6vcpvcr3vvf4qkhppgy56urmjcj2vagu2iqgp3z656xcmfdbiqd.onion
- ***Graph Tips***
  https://graph.tips/beta/
- **Whopostedwhat**
  https://www.whopostedwhat.com/
- ***Instant Data Scraper***

https://chrome.google.com/webstore/detail/instant-data-scraper/ofaokhiedipichpaobibbnahnkdoiiah

- ***Dumpitblue+***

  https://chromewebstore.google.com/detail/dumpitblue+/igmgknoiooooacbcpcfgjigbaajpelbfe

- ***FBDOWN.net***

  https://fdown.net/

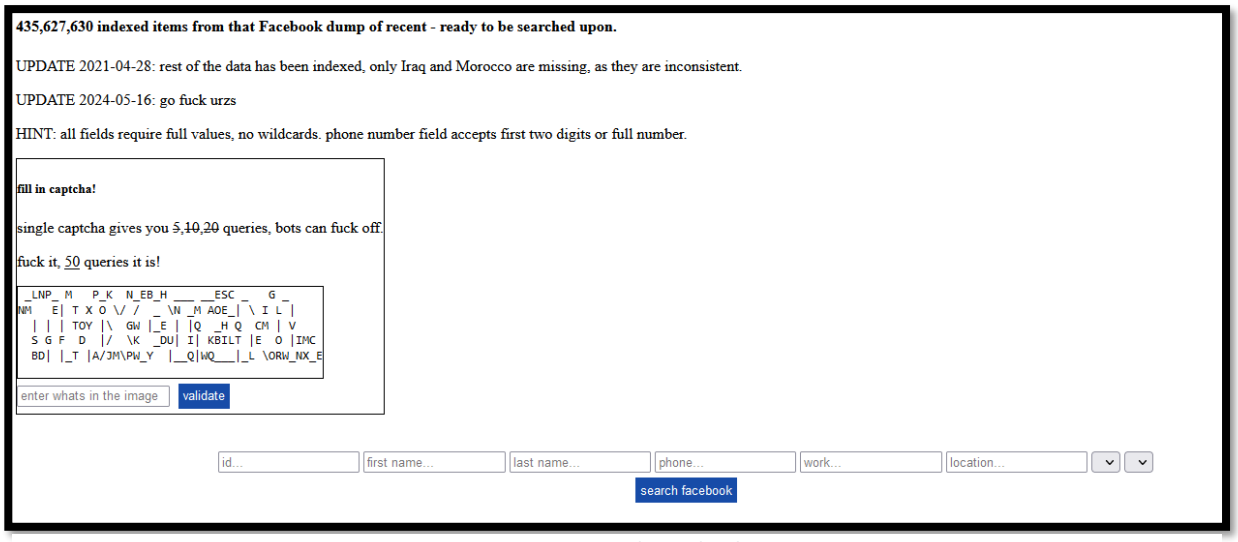


Figura 20:- Fuck Facebook

10.6.2. INSTAGRAM

Il secondo social network di META che possiamo usare per la ricerca e raccolta d'informazioni è Instagram.

Tuttavia, non è semplice come Facebook ricavare le informazioni, questo perché le restrizioni di *privacy* usate dagli utenti sono maggiori.

Tuttavia, come per Facebook, tra le informazioni che possiamo ricavare c'è:

- *Nickname e nome e cognome dell'utente;*
- *Dati anagrafici se indicati;*
- *Contatti (tramite le reazioni alle foto o guardando i follower e following);*
- *Reti di amicizie ed eventuali parenti;*
- *Informazioni come hobby e viaggi;*
- *Geolocalizzazione delle foto sia tramite l'impostazione dell'utente che tramite Il contesto dell'immagine;*
- *I vari tag di altri profili nelle proprie foto.*

TOOLS INSTAGRAM

Tra i vari tools che possiamo usare e attualmente funzionanti abbiamo:

- ***Picuki***
  https://www.picuki.com
- ***Storiesing.info***
- *https://storiesig.info/en/*
- ***Exportcomments***
  https://exportcomments.com/
- ***IG Follower Export Tool***
  https://chromewebstore.google.com/detail/strumento-di-esportazione/kicgclkbiilobmccmmidfghnijgfamdb
- ***IG E-mail Scraper***
  https://chromewebstore.google.com/detail/ig-email-scraper-extracto/cmlfhilehabkgmicijgaonjgdkiclcna
- ***Instaloader***
  https://instaloader.github.io

10.6.3. LINKEDIN

Questa piattaforma social è usata principalmente dai professionisti di ogni settore per la ricerca occupazionale ma anche dal network professionale di ogni settore. Questo va da sé che fa di questo social un enorme potenzialità in termini di dati sia per la ricerca dei membri di un'organizzazione sia per le informazioni personali legate al singolo utente.

Prima di iniziare a vedere quali sono i dati che si possono estrapolare dal singolo target, vediamo prima come possiamo impostare il nostro profilo *fake* in modalità *stealth.* Questo perché il social per sua natura, tende a far interagire gli utenti in modo da creare reti professionali. Ma il nostro scopo è il monitoraggio e la raccolta delle informazioni, senza che l'utente ne abbia percezione. Di seguito i diversi passaggi per l'impostazione del profilo:

- Andiamo sull'icona in alto "TU"
- Impostazioni e *privacy*
- Visibilità

- E cambiamo le impostazioni sia della "**visibilità del tuo profilo e rete**" che della "**visibilità della tua attività su Linkedin**" così come riportato nelle due foto in allegato (Figura 13)

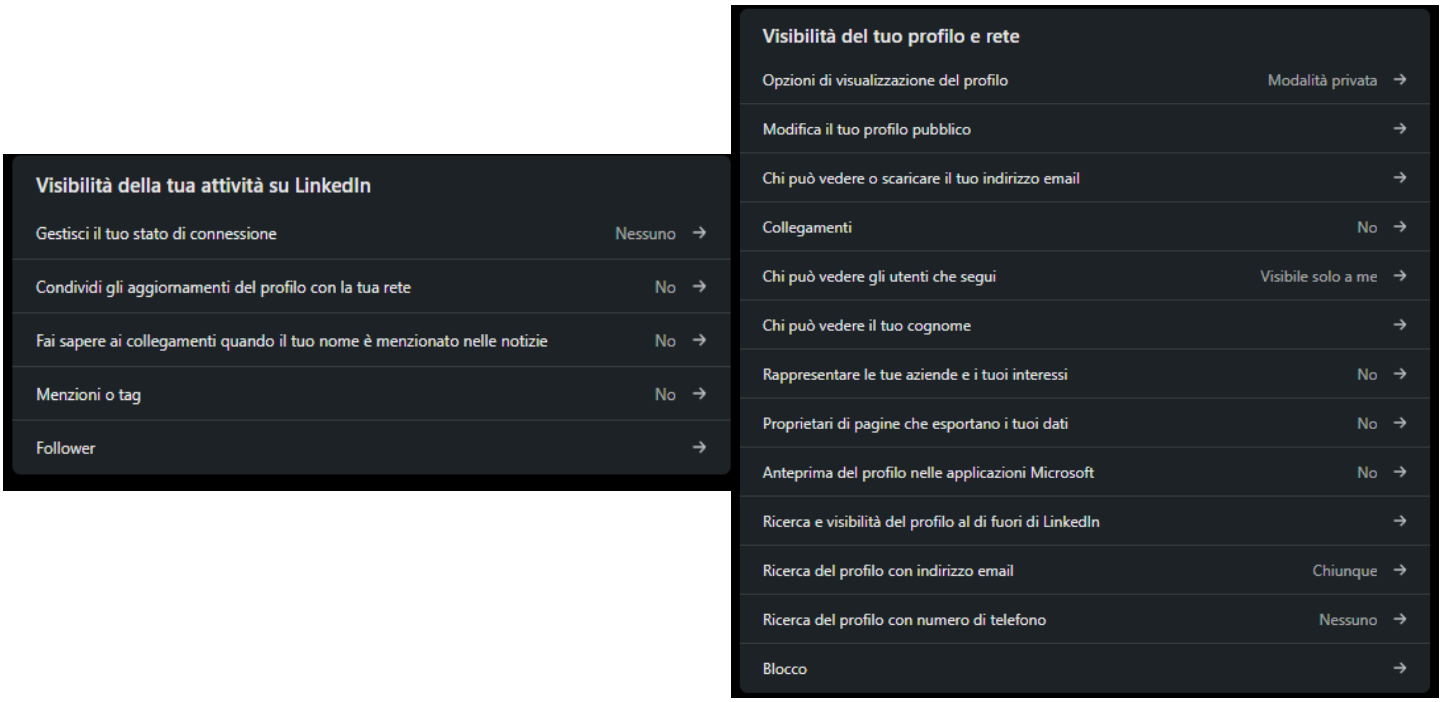


Figura 21:- Impostazione Privacy del profilo LinkedIn

Una volta impostato il nostro profilo, passiamo alla raccolta delle informazioni che possiamo reperire sui vari profili di LinkedIn. Tra le varie informazioni abbiamo:

- Nikname nella "Urls";
- Nome e cognome;
- Immagine del profilo;
- Professione ed esperienze lavorative;
- Biografia;
- Data di creazione del profilo;
- Numero follower e seguiti;
- Post e attività pubblicate.

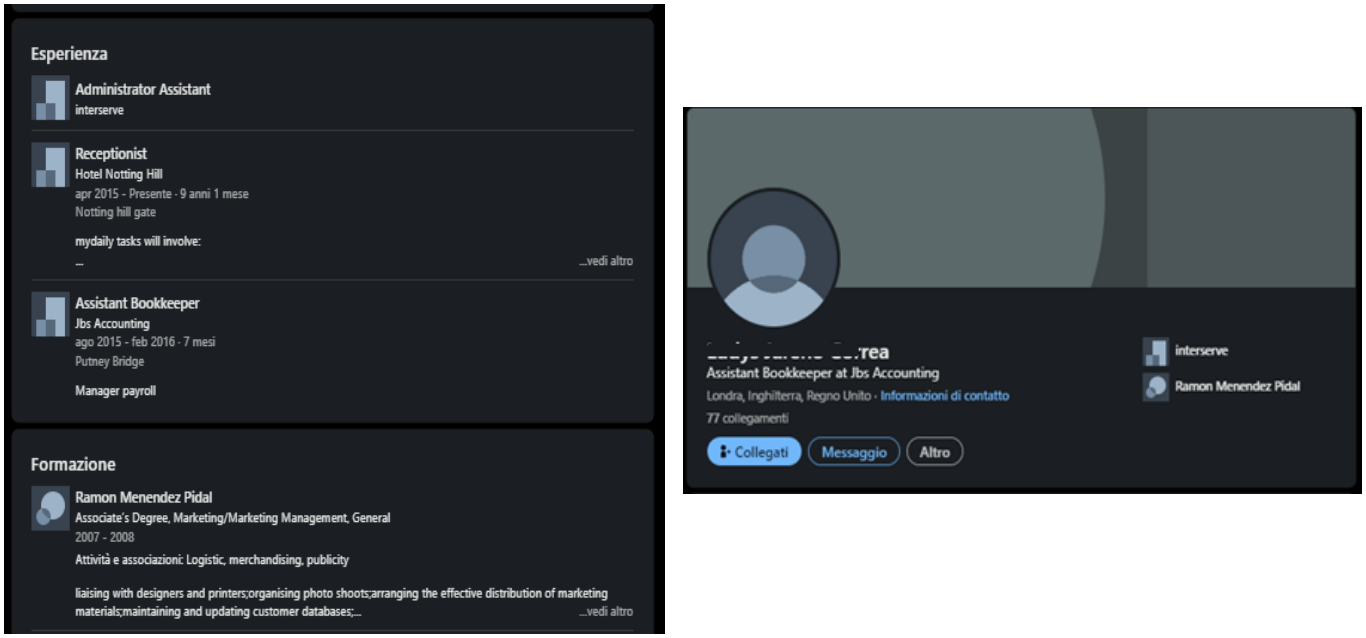


Figura 22:- Informazioni pubbliche all'interno del profilo LinkedIn

Se vogliamo cercare invece i membri di un'intera organizzazione, possiamo usare la barra di ricerca ed impostare i vari filtri in modo da ottimizzare la ricerca. In questo modo come risultato avremmo tutti gli utenti che tra le loro informazioni inserite nei propri profili, ci sia come esperienza lavorativa o lavoro in atto, il nome dell'organizzazione che noi abbiamo inserito.

Nell'esempio in allegato (Figura 15), abbiamo cercato tutti gli utenti che lavorano o hanno lavorato per ENI S.p.A.

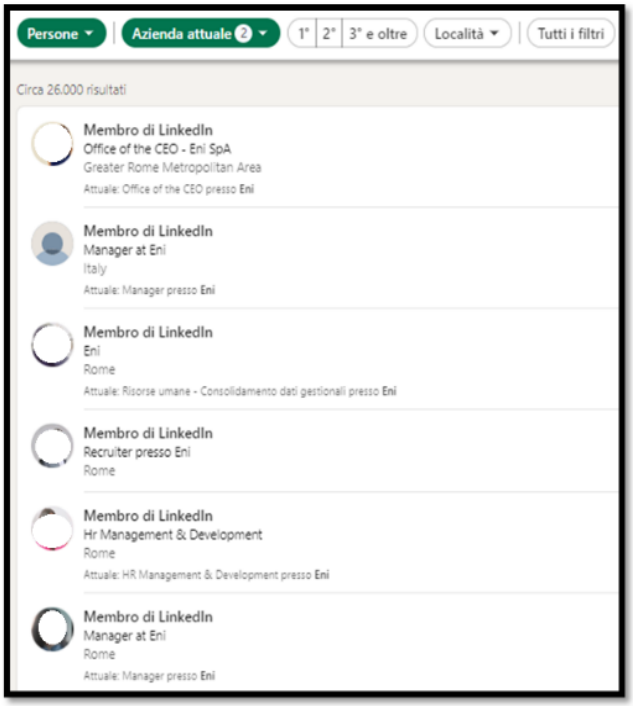


Figura 23:- Esempio di ricerca di membri di ENI SpA

TOOLS LINKEDIN

Tra i vari strumenti che possiamo utilizzare su LinkedIn vi è:

- ***Expertsphp***

  https://www.expertsphp.com/linkedin-video-downloader/
- ***Rocket Reach***

  https://chromewebstore.google.com/detail/rocketreach-chrome-extens/oiecklaabeielolbliiddlbokpfnmhba
- ***SignalHire***

  https://chromewebstore.google.com/detail/signalhire-find-email-or/aeidadjdhppdffggfgjpanbafaedankd

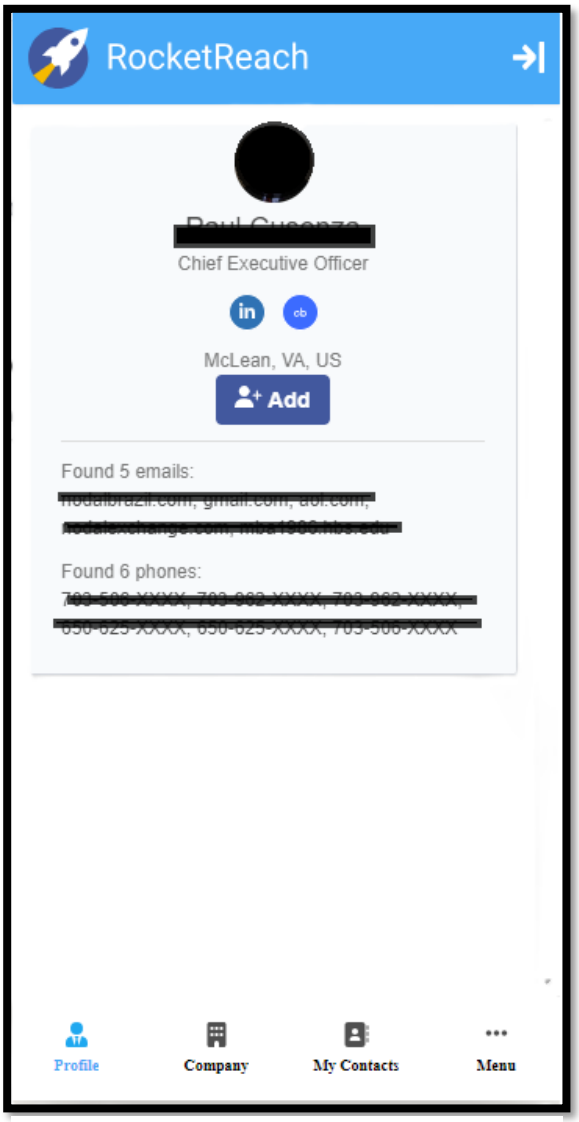


Figura 24:RocketReach

10.6.4. TWITTER/X

Twitter, oggi "X" dopo l'acquisizione di Elon Musk nell'aprile del 2022. È un social molto usato dagli utenti per esprimere opinioni, seguire tendenze etc. Grazie a questo si presta a molte analisi e raccolta d'informazioni. In particolare, è possibile monitorare i trend di un argomento grazie all'utilizzo degli utenti di hashtag nei loro tweet. In più tramite dei strumenti che successivamente verranno elencati, è possibile anche stabilire una geolocalizzazione dei "*trend*" oppure capire la personalità di un profilo etc. Ovviamente tramite la ricerca avanzata e l'uso di vari filtri, è possibile migliorare la ricerca dei singoli post o profili utente.

Nell'esaminare il profilo di utente possiamo ricavare le seguenti informazioni:

- *Analisi del nome utente (che può corrispondere anche ad un nikname usato in un altro profilo social o forum);*
- *Biografia se presente;*
- *Controllare data di creazione del profilo;*
- *Numero di following e follower;*
- *Lettura dei tweet anche storici, notando anche eventuali collegamenti ad altri siti web o social network e relativi hashtag;*
- *Infine, foto profilo e foto sfondo, quindi OSINT Image.*

Figura 25:- Twiiter/X

TOOLS TWITTER/X

Tra gli strumenti che possiamo usare di Twitter principalmente per il monitoraggio e l'analisi dei tweet, abbiamo:

- ***Foller***
  https://foller.me/
- ***Thread Reader App***
  https://threadreaderapp.com/
- ***Twiangulate***
  https://twiangulate.com/search/
- ***Get day Trends***
  https://getdaytrends.com
- ***One Million Tweet Map***
  https://onemilliontweetmap.com
- ***Download Twitter Video***
  https://www.downloadtwittervideo.com/

10.6.5. TELEGRAM

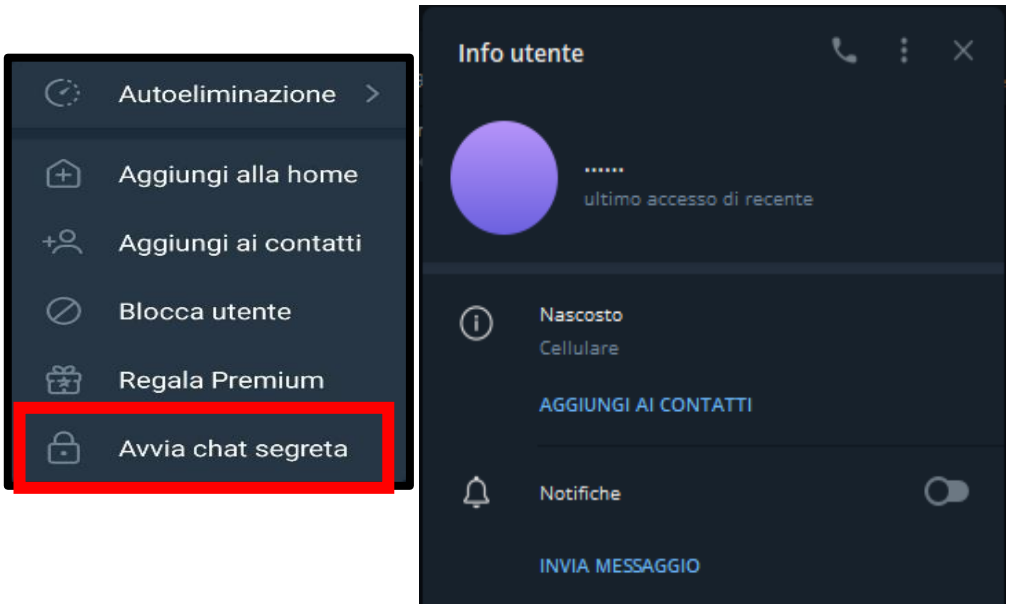
Telegram è un app di messaggistica usata e diffusa in tutto il mondo per le sue robuste opzioni di *privacy* e sicurezza. Di fatti viene utilizzata da molte organizzazioni criminali di vario tipo, per lo scambio di dati e non solo.

- Tra le caratteristiche dei singoli utenti abbiamo:
    - Foto profilo;
    - Nickname;
    - Biografia.

Queste informazioni però possono essere omesse dal singolo utente, rendendo difficoltoso per l'operatore OSINT l'attività di ricerca d'informazioni. Infatti, è possibile trovare dei profili che non rilasciano alcuna informazione utile per il riconoscimento.

- Tra le principali caratteristiche della piattaforma di messaggistica abbiamo:

- **Chat segrete con criptografia end-to-end:** alcune chat possono essere impostate in maniera criptografica in modo che le conversazioni sono visibili solo determinati dispositivi e quindi dagli utenti membri della chat.



- **Canali e gruppi pubblici e privati**: gli utenti possono creare e/o unirsi a diversi canali e gruppi sia pubblici che privati. La differenza sta nel fatto che i canali sono usati per la diffusione di notizie e contenuti e vi è un dialogo con i membri. Nel gruppo invece abbiamo lo scambio di messaggi e dati tra i membri appartenenti.
- **BOT di Telegram**: permette agli sviluppatori e amministratori di gruppi e canali di eseguire e automatizzare la gestione di task e servizi all'interno dei gruppi e non solo.
- **API per sviluppatori:** le API di Telegram permettono quindi di creare queste applicazioni e servizi che interagiscono direttamente con la piattaforma.

Di seguito indicheremo i servizi Web che ci danno un supporto per la ricerca e l'analisi dei gruppi Telegram e dei BOT più usati per l'attività di ricerca, analisi e monitoraggio di gruppi e profili Telegram.

Figura 26:- BotFather

TOOLS Telegram

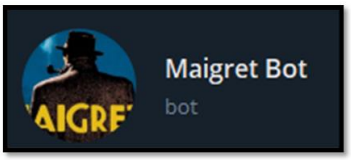
Tra gli strumenti che possiamo usare per la ricerca di gruppi e canali e il monitoraggio delle informazioni abbiamo:

Figura 27:- Telemetryapp.io

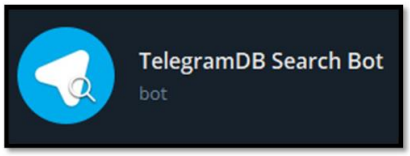
- ***Telemetryapp*** **-** *https://www.telemetryapp.io*
- ***Telegram Search Engine*** **-** *https://xtea.io/*
- ***TelegramGroup*** **-** *https://www.telegram-group.com/*
- ***Telegram Directory*** **-** *https://tdirectory.me/*
- ***TelegramDB*** **-** *https://www.telegramdb.org/search*
- ***TgStat*** **-** *https://tgstat.com/*
- ***Telegram-italy*** **-** *https://telegram-italy.it*
- ***Lyzem*** **-** *https://lyzem.com*

Oltre a questi strumenti esistono come abbiamo accennato prima, i BOT. Di questi ne segnaliamo alcuni che possono essere di supporto durante la fase di raccolta ed analisi dei profili e canali Telegram.

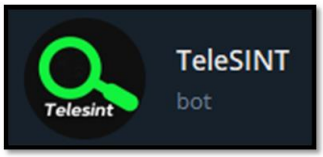
- *https://t.me/maigret_s2_bot* (***Ricerca username***)
- *https://t.me/tgdb_bot* (***Ricerca gruppi legati***)
- *https://t.me/telesint_bot* (***Ricerca ID Telegram***)
- *https://t.me/Quick_OSINTbot* (***Ricerca info su profilo***)
- *https://t.me/holehe_s_bot* (***Ricerca info e-mail***)
- *https://t.me/ooSearchBot* (***Ricerca gruppi, canali e BOT***)
- *https://t.me/TrueCaller_Z_Bot* (***Ricerca nominativo da numero di telefono***)



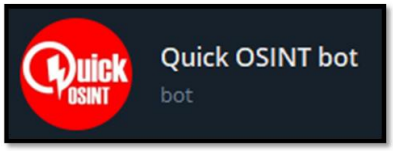
https://t.me/maigret_s2_bot



https://t.me/tgdb_bot

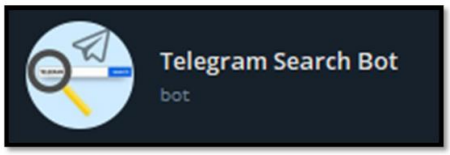


https://t.me/telesint_bot



https://t.me/Quick_OSINTbot

https://t.me/holehe_s_bot



https://t.me/ooSearchBot

11. ANALISI DEGLI USERNAME/NOME REALE

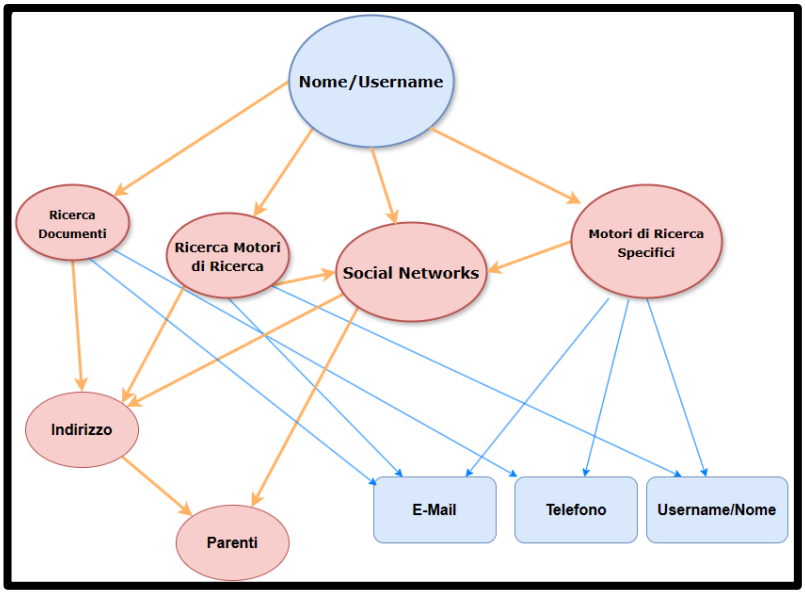


Figura 28:- Flowchart Analisi Username

La ricerca tramite il vero nome di una persona può essere faticosa e frustrante. Se il tuo obiettivo ha un nome comune, è facile perdersi nei risultati. Anche un nome abbastanza unico produce quasi 20 indirizzi, profili e numeri di telefono di persone. Se il nostro obiettivo si chiama *"Marco Rossi"* (un nome completo comune italiano), abbiamo un problema. Questo è il motivo per cui dovremmo preferire la ricerca per indirizzo email o numero di telefono quando disponibile. Ciò rientra tra le prime attività da svolgere al fine di cercare nome e cognome che ci interessa sui principali motori di ricerca, come Google, Yandex o Duckduckgo. Ma se vogliamo ottimizzare la ricerca ed individuare eventualmente documenti specifici come concorsi pubblici o curriculum vitae, possiamo utilizzare le Google Dorks oppure andare nei principali social network di cui abbiamo parlato nei capitoli precedenti.

Questi sono alcuni strumenti che possiamo utilizzare per effettuare ricerche conoscendo solo nome, cognome o username.

- **Whatsmyname** - https://whatsmyname.app
- **Namechk** - https://namechk.com
- **Usersearch.org** - https://usersearch.org
- **FuckFacebook** https://4wbwa6vcpvcr3vvf4qkhppgy56urmjcj2vagu2iqgp3z656xcmfdbiqd.onion
- **Webmii** - https://webmii.com
- **Castrick** - https://castrickclues.com/

12. GOOGLE DORK

Le Google Dork sono “query” di ricerca avanzata che possono aiutare a trovare dati specifici o nascosti nel motore di ricerca Google. Ma possono essere anche utilizzate per recuperare dati sensibili oppure identificare vulnerabilità etc.

Ad esempio, potresti essere in grado di trovare il curriculum vitae di una persona o la dichiarazione dei redditi di un’azienda, le note spese di un’amministrazione comunale, documenti relativi a concorsi pubblici con i dati anagrafici dei partecipanti. Dettagli che potrebbero non essere visualizzati sui loro siti Web o visualizzati quando esegui una ricerca web di routine.

Di seguito riportiamo un elenco di alcune Google Dork[3] che possono essere usate per la ricerca di documenti:

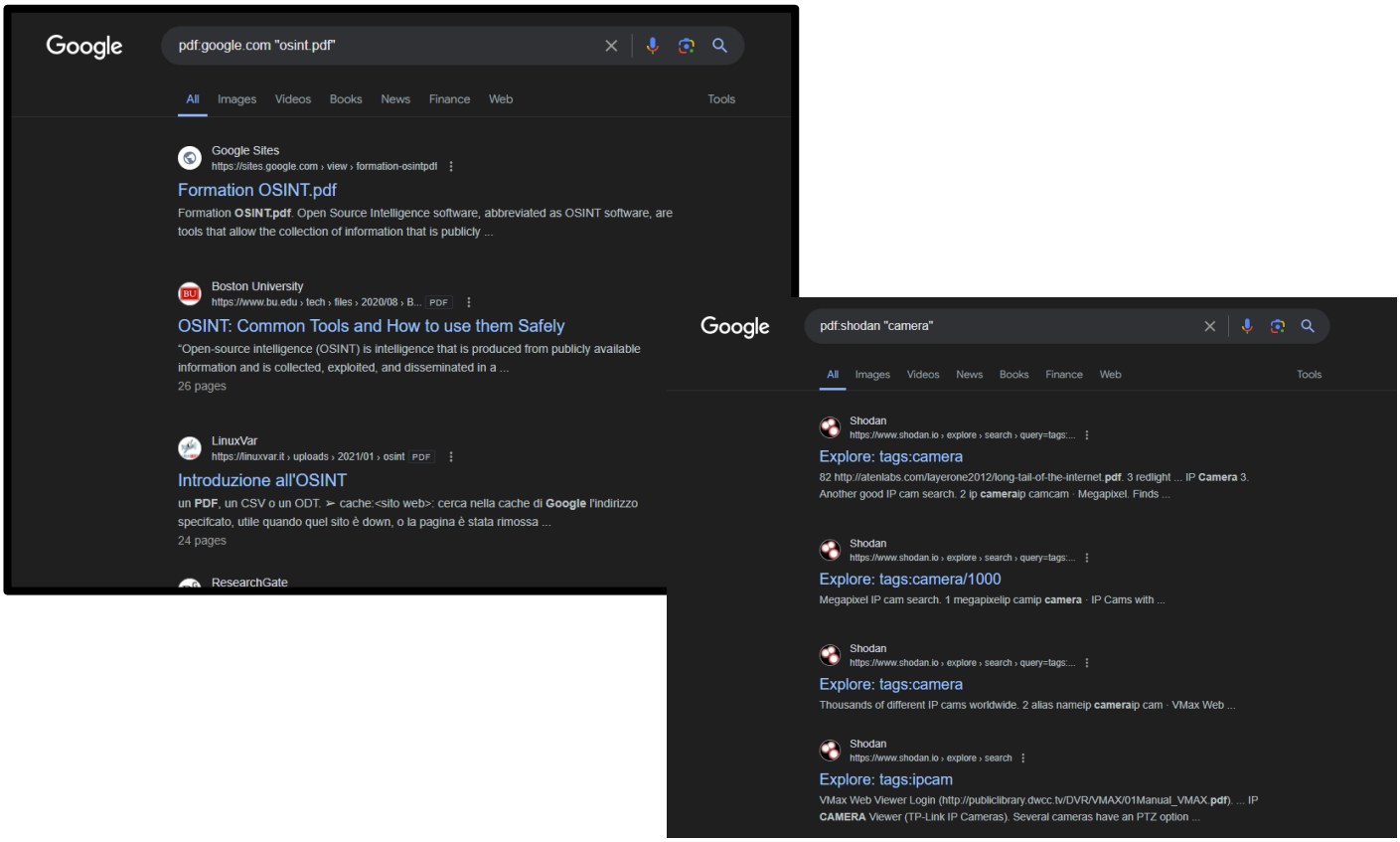


Figura 29:- Esempio di ricerca usando le Google Dork

[3] Oltre agli strumenti sopra elencati, di seguito seguendo questo link https://github.com/CScorza/OSINTInvestigation/blob/main/-%207000%20-%20Google%20Dork.txt è possibile trovare più di 7000 google dork che possono essere usate per la ricerca di diversi scopi più specifici.

Ricerca generale di PDF	site:example.com filetype:pdf
Ricerca di PDF con titoli specifici:	intitle:"argomento desiderato" filetype:pdf
Ricerca di CV:	intitle:cv | "curriculum vitae" filetype:pdf | filetype:doc
Ricerca di CV per area geografica o competenza:	intitle:cv "ingegnere" | "developer" | "designer" location:italy filetype:pdf | filetype:doc
Ricerca di CV in siti specifici:	site:linkedin.com | site:indeed.com "curriculum vitae" | cv filetype:pdf | filetype:doc

Se vogliamo utilizzare qualcosa che ci facilità ad usare le *Google Dork*, possiamo usare le seguenti pagine web, che ci permettono di effettuare delle ricerche più puntuali:

- **CScorza Search** - https://cse.google.com/cse?cx=d28c23ec014bd4cca - gsc.tab=0
- **DorkGPT** - https://www.dorkgpt.com/
- **Eye of Justice** http://eyeofjustice.com/od/
- **Analyst Research Tools** https://analystresearchtools.com/
- **Dork Search**: https://dorksearch.com/
- **Open Directory Finder** https://ewasion.github.io/opendirectory-finder/

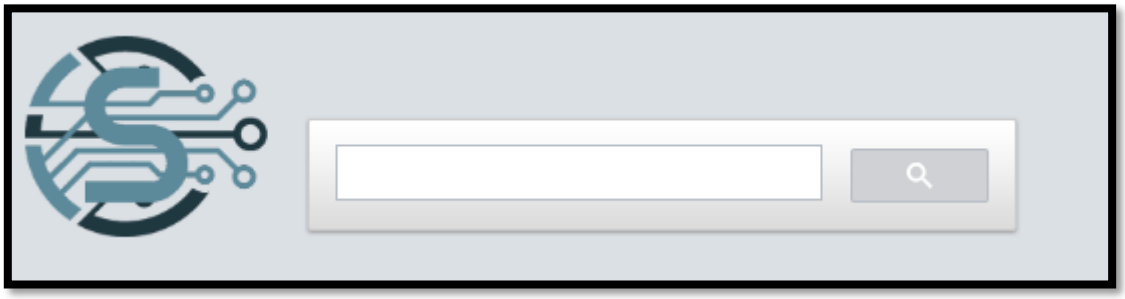


Figura 30:- CScorza Search

13. ANALISI DELLE E-MAIL

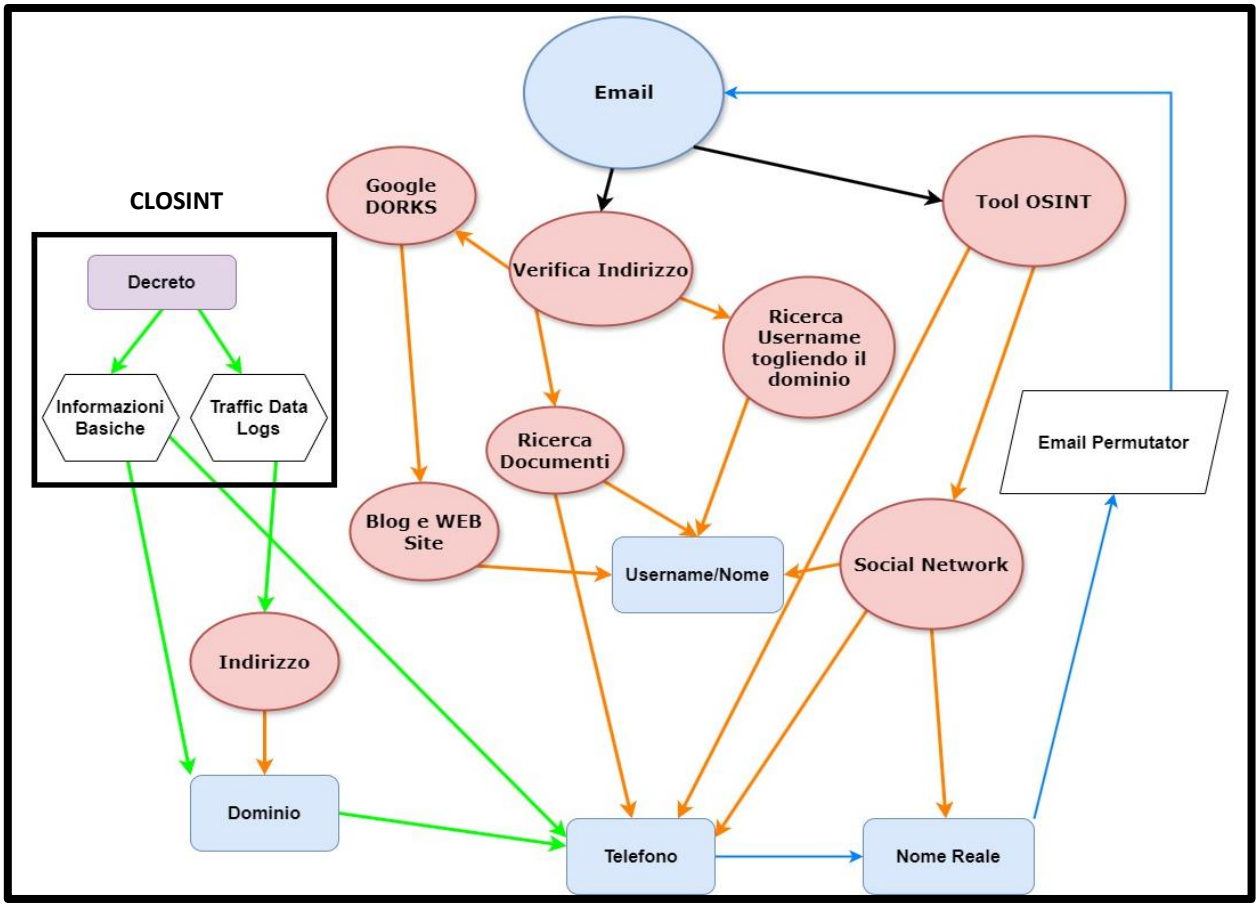


Figura 31:- Flowchart Analisi e-mail

Ci può capitare di conoscere l'indirizzo email del nostro obiettivo e vogliamo capire a quali servizi è collegato in modo da ottenere le informazioni reali del nostro target come, nome e cognome e numero di telefono, etc.. Come si può evincere dal flow chart (Figure 21), possiamo eseguire diversi passaggi per raggiungere il nostro scopo, tra cui le "Google Dork" come abbiamo visto in precedenza ma anche l'uso di strumenti OSINT gratuiti o a pagamento che ci possono fornire una serie di risultati per noi utili. Tra i vari tool che possiamo usare per effettuare queste tipo di verifiche abbiamo:

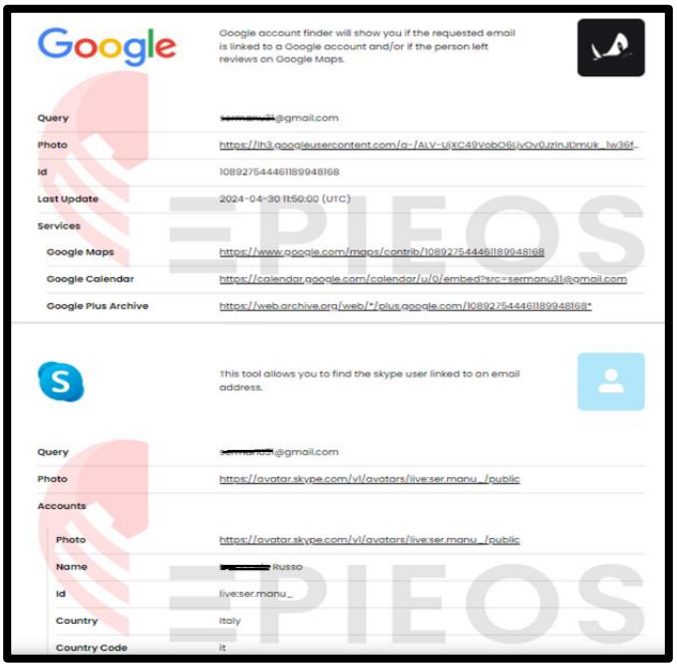


Figura 32:- Epieos

- **Seon.io** - *https://seon.io*
- **Castrickclues.com** - *https://castrickclues.com*
- **Dehashed** - *https://www.dehashed.com*
- **Epieos** - *https://epieos.com*
- **Espysys** - *https://www.espysys.com*

Di fatto questi strumenti offrono la possibilità di verificare a quali social network o servizi web l'email è inserita, riuscendo a fornire ulteriori dati come il nome e cognome e l'immagine profilo (vedi Figure 21).

14. ANALISI NUMERO DI TELEFONO

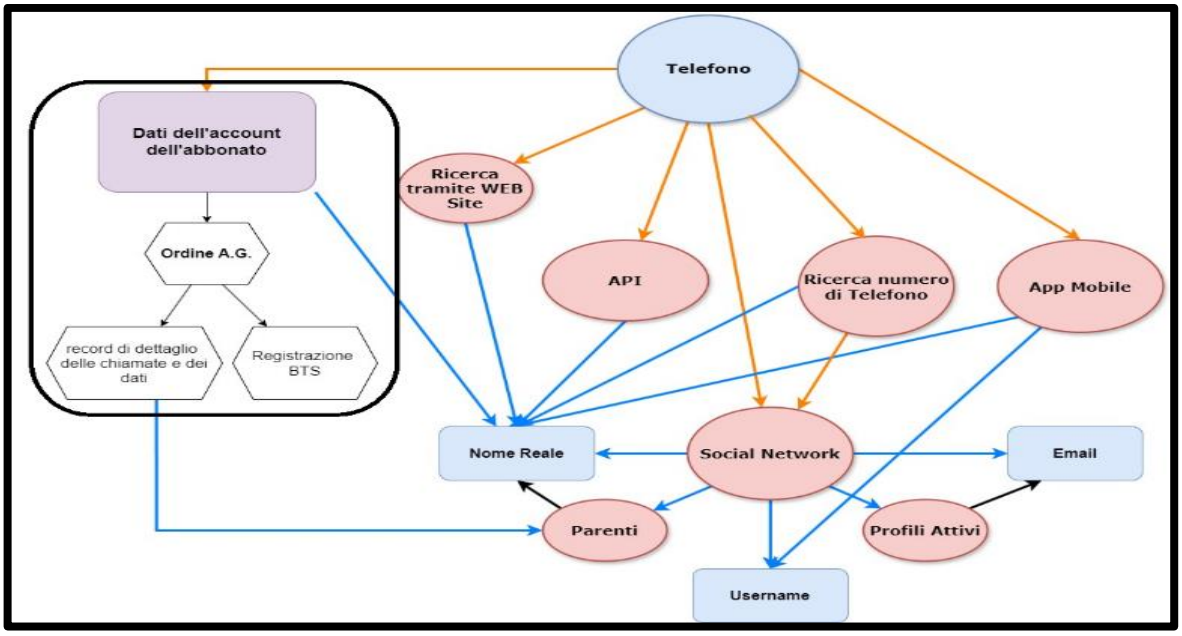


Figura 33:- Flowchart Analisi numero di Telefono

Se disponiamo di un numero di telefono, possiamo effettuare tre attività per la ricerca del suo utilizzatore:

1. Identificare che tipo di numero è ed il suo fornitore; quindi, capire se ci troviamo di fronte ad un numero di telefono fisso o cellulare o di tipo "dati". Inoltre, capire il fornitore se è locale o estero.
2. Identificare qualsiasi informazione dell'utilizzatore come nome e cognome ed eventuale indirizzo di residenza ed e-mail associata.
3. Infine, possiamo ricercare i vari servizi che sono direttamente collegati al numero di telefono, come app di messaggistica (WhatsApp, Telegram), social network etc. Tutto

ciò porterà inevitabilmente ad ulteriori informazioni che ci possono essere d'aiuto per ampliare la nostra ricerca.

Esistono diversi tool che possono essere usati, per fare delle analisi dei numeri di telefono, alcuni di questi li abbiamo già incontrati in precedenza, come **OSINT Industries, Epeios** e **Castrick**.

Oltre a questi esistono altri strumenti che ci permettono l'analisi di un numero di cellulare come:

- **CallApp** - https://callapp.com
- **SyncMe** - https://sync.me
- **Truecaller** - https://www.truecaller.com

Queste applicazioni[4] permettono di effettuare delle ricerche su qualunque numero di telefono mobile rilasciando come informazione il nome del suo utilizzatore. Inoltre, danno anche la possibilità di verificare se il numero di telefono è registrato nelle piattaforme di messaggistica più comuni come WhatsApp.

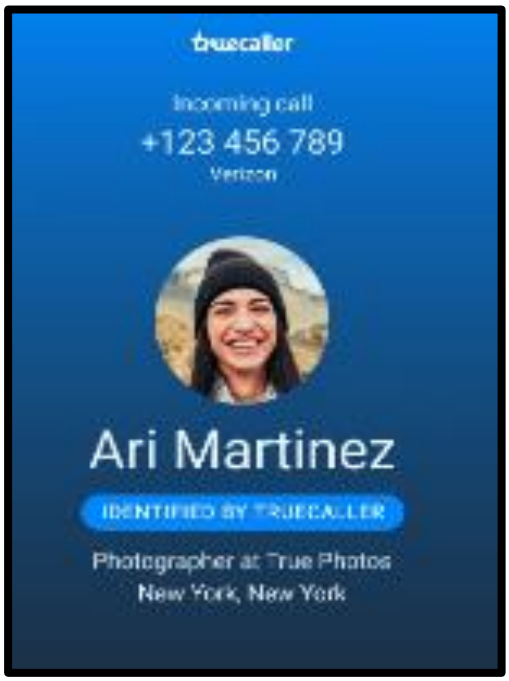


Figura 34:- Truecaller

[4] Importante da notare che queste applicazioni richiedono l'accesso alla rubrica del proprio telefono. Quindi è opportuno usare queste applicazioni con cautela, attraverso per esempio l'utilizzo di un VM Android, Android Studio, oppure un telefono vecchio senza numeri di telefono salvati in rubrica.

CONCLUSIONI

Nel corso di questo manuale, abbiamo esplorato in dettaglio l'Open Source Intelligence (OSINT), un campo dinamico e in continua evoluzione. Abbiamo iniziato con una panoramica storica, che ci ha fatto capire quanto da sempre sia stato nel corso del tempo importante raccogliere dati ed informazioni per le varie nazioni. Abbiamo anche delineato le varie branche dell'OSINT e l'importanza nel contesto moderno.

Abbiamo distinto tra OSINT Attivo e Passivo, evidenziando le tecniche e gli strumenti di monitoraggio utili per ciascuna modalità. Successivamente, abbiamo approfondito il "Metodo Pivoting", un processo fondamentale per l'efficace flusso di lavoro OSINT, permettendo di muoversi agevolmente tra diverse fonti di informazione per costruire un quadro completo e accurato e inserirlo nel report finale.

La distinzione tra *Clearweb* e *Deepweb* ci ha permesso di comprendere meglio dove operare e come accedere a informazioni meno visibili ma altrettanto rilevanti ed importanti. Abbiamo esaminato l'uso e l'installazione di una VPN per garantire non solo la sicurezza e anonimato utili per la protezione dei nostri dati, ma anche migliorare la ricerca delle informazioni.

L'importanza di una gestione delle password, strumento indispensabile per mantenere al sicuro le credenziali di accesso.

La creazione di una Workstation dedicata, così come la scelta di sistemi operativi adeguati tra Linux, Windows e Mac, sono passaggi cruciali per stabilire un ambiente di lavoro sicuro ed efficiente.

Abbiamo poi esaminato i browser ed i motori di ricerca, con un focus particolare su Tor Browser, Mozilla Firefox e Brave, e l'uso di estensioni per migliorare la privacy e la sicurezza durante la navigazione, oltre che per raccogliere dati durante la nostra navigazione.

La sezione sulla Social Media Intelligence (SOCMINT) ha fornito una guida dettagliata sulla creazione di avatar (sockpuppet) per l'infiltrazione e la raccolta di informazioni nei social network, coprendo vari aspetti come la biografia, l'immagine del profilo, l'e-mail e il numero di telefono.

Inoltre, ci siamo soffermati sull’esplorazione di specifiche piattaforme come Facebook, Instagram, X/Twitter, LinkedIn e Telegram, evidenziando le tecniche per sfruttarle al meglio.

L'analisi degli username e dei nomi reali, insieme all'uso delle Google Dork, ha mostrato come estrarre informazioni preziose attraverso ricerche avanzate.

L'analisi delle e-mail e dei numeri di telefono ha completato il quadro degli strumenti disponibili per una ricerca OSINT efficace.

In conclusione, questo manuale fornisce una guida comprensiva e pratica per chiunque desideri avvicinarsi al mondo dell'OSINT. Conoscere e saper utilizzare queste tecniche non solo amplia le nostre capacità di raccolta di informazioni, ma ci prepara anche a navigare nel complesso panorama digitale con maggiore sicurezza e consapevolezza.

BIBLIOGRAFIA

- *"Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information" di Michael Bazzell*
- *"Deep Dive": Exploring the Real-world Value of Open Source Intelligence 1st Edition*
- *Vari corsi seguiti online.*
- *Aggiornamento costante*
- *Confronto costante con altri analisti OSINT e d'Intelligence.*

Tutti gli esseri umani hanno tre vite: pubblica, privata e segreta.

- **Gabriel García Márquez**

“CScorza”

Esperto in Tecniche e Metodi di Open Source Intelligence.
Tramite il profilo GitHub e il Canale Telegram aperti nel 2022, raccoglie software e strumenti di OSINT, Digital Forensics e Cyber Security.
All’interno del suo canale Telegram “CScorza – Indagini Telematiche”, tiene aggiornati i suoi repository di GitHub con le nuove tecniche e strumenti di oltre 20 tematiche diverse.