CSCORZA

Open Source Intelligence Basic Manual

BASIC MANUAL OF

OPEN SOURCE INTELLIGENCE

Text written and produced by**CScorza**

Year of publication 2024

Contacts:

Linkedin: https://www.linkedin.com/in/cscorza

Tweet/X: https://x.com/CScorzaOSINT

Telegram: https://t.me/CScorzaOSINT - *"CScorza – Telematic Investigations"*

GitHub: https://github.com/CScorza https://www.lab4int.org

LAB4INT:

INDEX

PREFACE

It is with great pleasure and honor that I present this "Basic Manual of Open Source Intelligence" written by CScorza. I had the privilege of personally knowing CScorza during the Digital Intelligence course, where he demonstrated not only extraordinary professionalism and competence, but also a remarkable aptitude in disseminating his knowledge on OSINT and anonymity, a fundamental principle of undercover investigations .

CScorza has done a commendable job, creating a manual that is aimed at both beginners and experts in the sector. His ability to transform complex concepts into accessible and useful information is a testament to his commitment and passion for the subject. This manual is not just a collection of techniques and tools, but a practical and theoretical guide that provides a complete overview of OSINT, from historical foundations to more advanced applications.

The manual explores in detail the different branches of OSINT, such as Social Media Intelligence (SOCMINT), and many others. Through well-structured chapters, CScorza guides us in the creation of dedicated workstations, in the use of VPNs and password managers, and in the advanced analysis of user agents. The section on creating avatars for infiltrating social networks is particularly useful for those who want to learn more about anonymity and identity protection techniques.

Collecting and analyzing information from publicly available sources is more crucial today than ever. We live in an age where the amount of accessible data is enormous, and the ability to extract useful information from this sea of data is an essential skill. CScorza, with this manual, offers us the tools and knowledge necessary to navigate this complex information landscape.

I want to emphasize that OSINT is an ever-evolving field. Techniques and tools that we consider cutting-edge today could quickly become obsolete. Therefore, continuous learning and constant updating are essential. This manual represents a fundamental starting point for anyone wishing to undertake this path, but should not be considered a point of arrival.

In conclusion, I praise CScorza's work for his dedication and for making his skills available to all of us. I am sure that this manual will become a valuable reference for many operators in the sector.

Welcome to the world of Open Source Intelligence!

Dr. Simone Bonifazi
President of LAB4INT

INTRODUCTION

If you are reading this manual, it means that you already know me and follow my Telegram channels as well as my GitHub page, where over the years I have put together a series of repositories that contain all the useful tools for browsing the web, for the collection and analysis of OSINT in many of its subclasses (e.g. SOCMINT, GEOINT, CORPINT etc.), Digital Forensics and OSINT Image, i.e. the analysis of images for the collection of information that may be useful for us to achieve the our goal. Given the incessant demand to create something that can help even those who are new to the world of OSINT, I started writing and putting together this manual, in order to capture the salient points for creating a "*basic workstation*", therefore a series of tools ranging not only from hardware to software, but also techniques and advice to begin our monitoring, collection and analysis of information accessible on the internet.

Let's start with two questions:

Do you need an OSINT manual? and what is OSINT?

To answer the first question, we must necessarily start from the second. OSINT, or Open Source Intelligence, is the collection and analysis of information from publicly available sources to support decision-making and intelligence operations. Due to its nature, it lends itself to government scenarios (law enforcement, armed forces and intelligence services) and private contexts.

The ability of a good analyst consists in transforming simple data, which may apparently seem trivial, into significant information. Therefore, this process is encapsulated in the intelligence cycle, which we will discuss in the next chapters. The effectiveness of a good analysis depends on the operator's ability to identify, access and analyze open sources and information, guaranteeing accuracy and relevance of the data collected. At this point to the question, whether "an OSINT manual is needed", the answer is "no", because there is no guideline that is suitable for any analyst, as each operator has his own cultural baggage made up of knowledge, IT skills and intelligence that can help and support him during the activity. Furthermore, each state has different regulations regarding the right to*privacy*and the processing of personal data, for this reason a good operator updates himself and studies the various places where he is carrying out his research, to find his data on public databases, social networks

most popular networks in a specific geographical area such as, for example, WeChat for China or Ok, VKontakte for Russia, etc.

It's true that you have to start from some basics, and here I tried to write something that is easy to use for anyone who enters this world.

Another element to take into consideration is Big Data. To date, every operator is inundated with hundreds of pieces of information, and it is up to the latter's ability to decide what to consider as useful data and then insert it into their report and what not. In this, OSINT gives us useful and necessary tools to be able to eliminate what is defined as "noise" or misleading information, bringing out only those that are intended to be included in our final report.

This manual was born from the courses and experiences acquired over the years in the field of OSINT. Since this industry is extremely dynamic, continuous updating is essential. Therefore, this manual does not represent the end of your journey, but rather a starting point or a further step forward in your continuous search for information.

At this point, Welcome to the world of Open Source Intelligence!!!

1. HISTORY OF OSINT AND ALL ITS BRANCHES

The first forms of information gathering can be traced back to ancient civilizations, where those responsible for war strategies (rulers and generals) relied on merchants, travelers and diplomats to obtain strategic information. The Romans and Greeks, for example, used this information to plan military campaigns.

During the Middle Ages, information gathering continued, with the collation of local chronicles, travel reports, and letters from missionaries and merchants. In fact, they were the connoisseurs of distant territories and could help understand the political and social dynamics of the different regions.

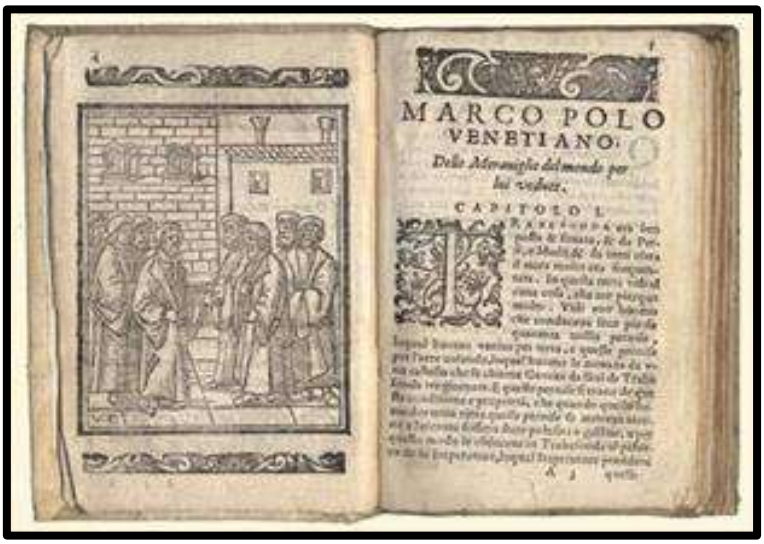


Figure 1:- The Million

With the advent of the printing press in the modern age, such news grew exponentially, newspapers became a crucial source of information for governments and military organizations, allowing them to monitor events in various regions and technological and political developments.

During the two World Wars, the use of information-gathering tools increased considerably. Through activities such as SIGINT (interceptions of radio transmissions), foreign press and other public sources, it was possible to gather strategic information. Governments used propaganda and counter-propaganda to influence public opinion.

Figure 2:- The Secret Intelligence Service (SIS)

Figure 3:- The Sicherheitsdienst

Figure 4:- The Office of Strategic Services (OSS) USA

The Cold War was characterized by ideological, military and economic competition between the US-led West and the USSR-led East. In this context, information gathering played a crucial role in the intelligence strategies of the two superpowers. Even if the information on the adversary was very limited, what could certainly help was the use of publicly accessible sources, such as political and security collection and analysis.

Figure 5:- KGB Committee for State Security - USSR

Figure 6:- CIA Central Intelligence Agency- US

With the digital age and the communications revolution, the amount of information has exploded, including forums, websites, social media and blogs. In this context, the possibility of accessing a vast range of data in real time has radically transformed the collection and analysis capacity. Thanks to scraping, data mining and social media analysis tools, OSINT activity has been made more efficient and precise. With these tools we can collect, filter and analyze large amounts of data. The importance of OSINT has also affected private interests as they can be useful for various purposes, such as

security of its infrastructures, risk analysis and therefore the protection of any threats. The subgroups that belong to OSINT are:

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

Together, these subgroups mean that the search for information is divided by sector of expertise and knowledge of the topic. However, everyone responds to four distinct phases:

- Discovery (*Discovery*) – Knowing who knows (*Know who knows*)
- Discovery (*Discrimination*) – Knowing “what is what” (*Know What's What*)
- Distillation (*Distillation*) – Knowing what is "relevant" (*Know What's hot*)
- Dissemination (*Dissemination*) - Knowing “who is who” (*Know Who's Who*)

This is because with the digital age there is multiple "information" on a single news story. Therefore it becomes important to be able to distinguish true "data" from false ones, or those important for investigative purposes from those of less operational interest.

2. ACTIVE OSINT AND PASSIVE OSINT (MONITORING)

It is important to distinguish these two activities in order not to fall into confusion when gathering information. In fact, based on the level of interaction we can have with the target, we can find ourselves operating a different type of activity.

So below we have:

- **PASSIVE OSINT**

  It consists of monitoring and collecting information on a specific target or groups, without any interaction. That is, there is a collection of data that is already publicly available without leaving traces of its presence or activity.

An example could be:

- or **monitoring a Facebook profile:**collecting photos, comments, personal information etc., without leaving a like, a comment or sharing a post on the target's wall;
- or **analysis of a website or blog:**reading articles, blogs without the site owner being aware of who is visiting the site; **search public databases:**
- or access to public records, archives or other databases that do not require interaction with the source.

- **OSINT ACTIVE**

  At this stage, we see that a form of interaction with information sources is present.

  For example, creating a fake profile or avatar (which we will address later) can be useful for registering on a social network, forum or even sending emails to access general information that is not indirectly connected. to criminal activity.

  However, Active OSINT should not be confused with Undercover or undercover agent activity, which is governed by a different rule than the collection of evidence sources and which requires a whole series of preliminary operations specific to this type of activity.

3. PWORKFLOW PROCESSESOSINT - "MMETHODPIVOTING"

In digital surveying, one of the most common questions is:

"There is a standard process or workflow for OSINT, SOCMINT and collection data in general?"

To answer this question, we should take into account that each investigation is unique, the cyberspace scenario is extremely dynamic (e.g. an end user or a social media that frequently changes its privacy policies*privacy*) and no "*cheat sheets*" can be used for any case. So, it might be a gamble to answer "*Yes*" to the question above. Anyway, we can use some kind of mind map based solution, which can quickly help with direction and guidance.

This solution considers six categories based on the information you are looking for, such as:

- **E-mail;**
- **Username or username;**
- **Telephone number;**
- **Domain name;**
- **Geolocation.**

Each of the following workflows should be considered when we are researching a chosen topic. For example:

- If you provide us with an email address, our goal is to find any usernames and real names;
- When we have a username, our goal is to find any social networks and verify an email address;
- When we have a real name, the goal is to find email addresses, usernames and phone numbers;
- When we have a phone number, our goal is to verify the name and identify a physical address and relatives;
- When we have a domain name, our goal is to identify a real name and address;

The cycle continues after each new piece of information is discovered.

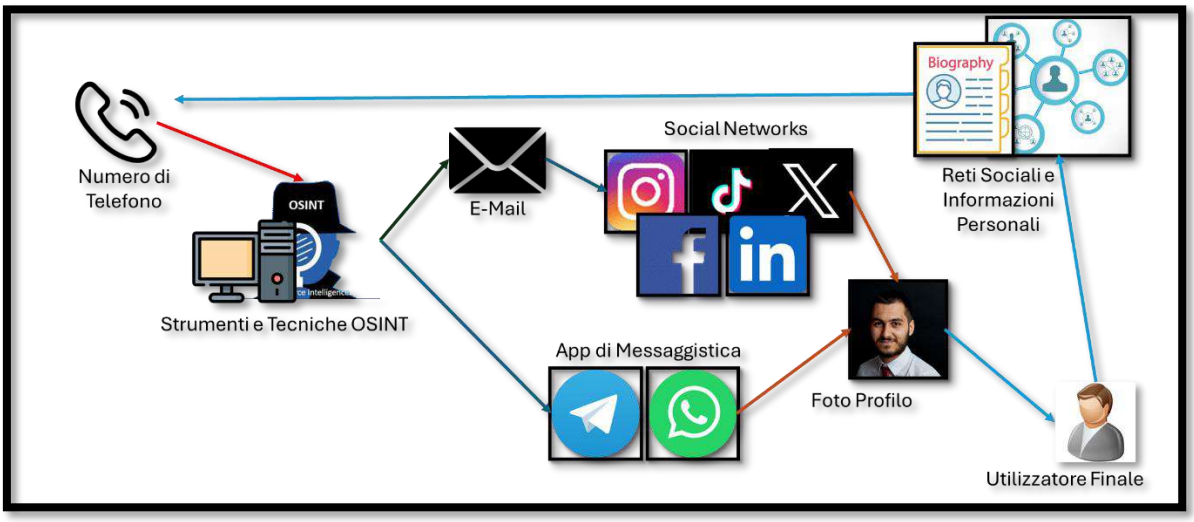


Figure 7:- Example of OSINT Activity

3.1. MMETHODPIVOTING

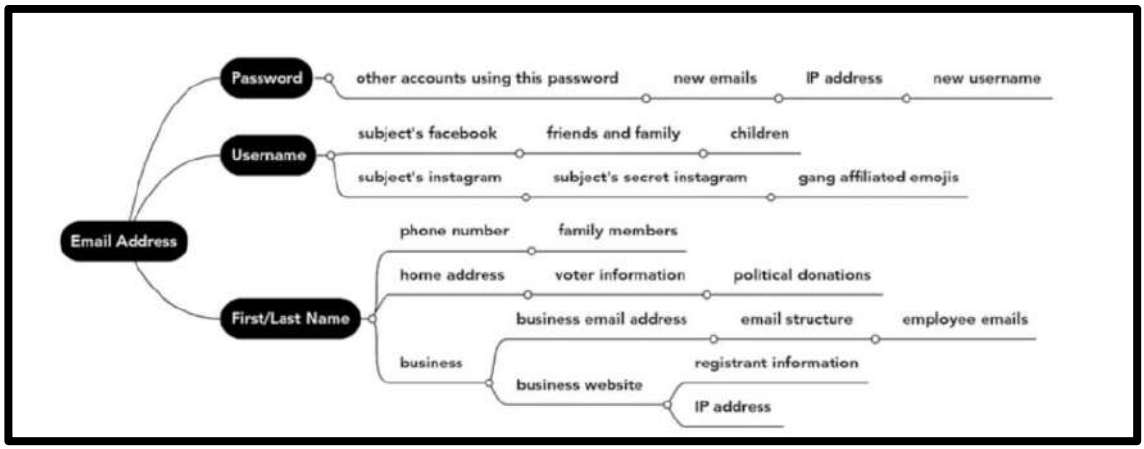


Figure 8:- Taken from the book DeepDive by Biker Wiley

The cycle we have described so far is called "*Pivoting method*" and is achieved by creating flowcharts that serve the individual operator to create a sort of guideline in the early stages of the intelligence cycle[1] or the collection of information.

[1] From a functional point of view, intelligence can be described as an information process defined by a cycle of actions divided into several phases (so-called "intelligence cycle") aimed at the general objectives identified by the government authorities (*https://www.sicurezzanazionale.gov.it/cosa-facciamo/analysis-intelligence*).

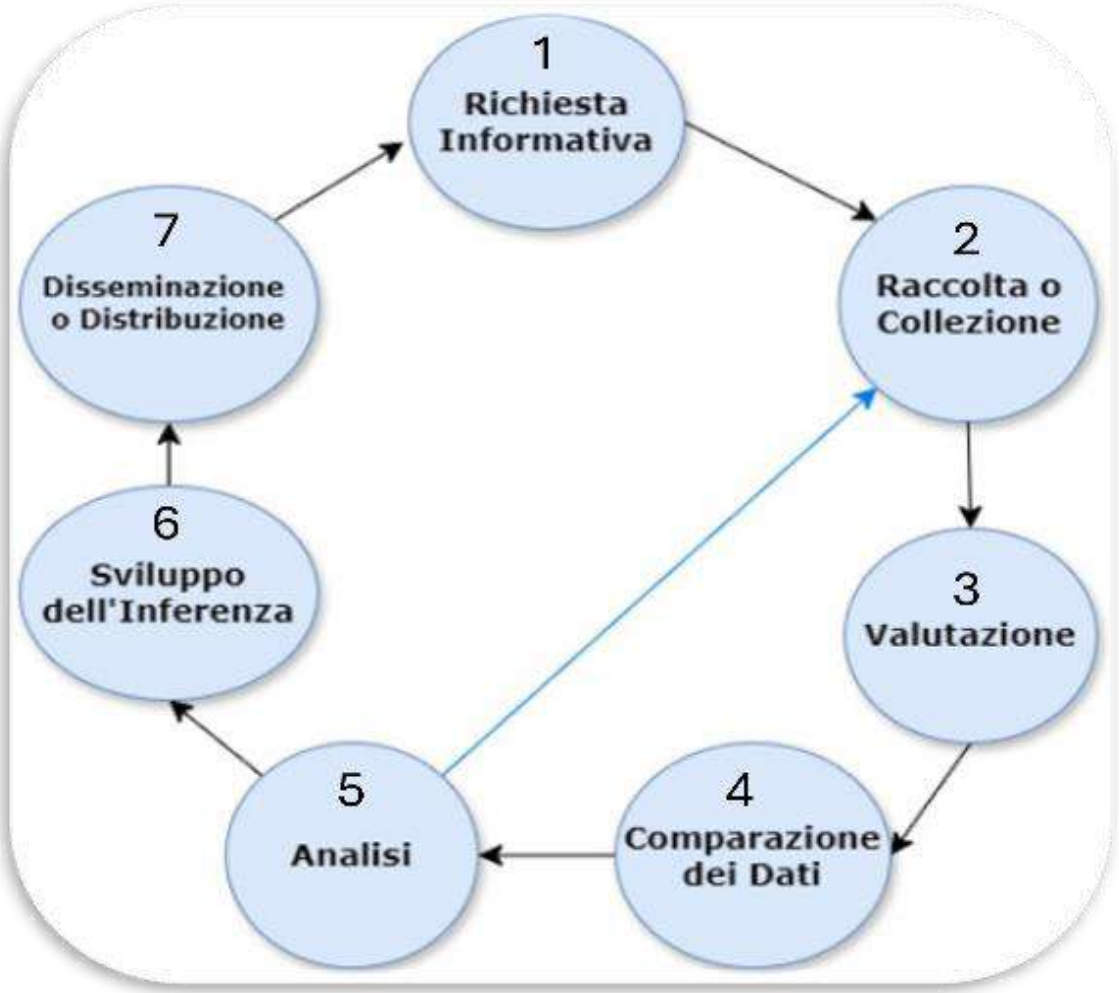
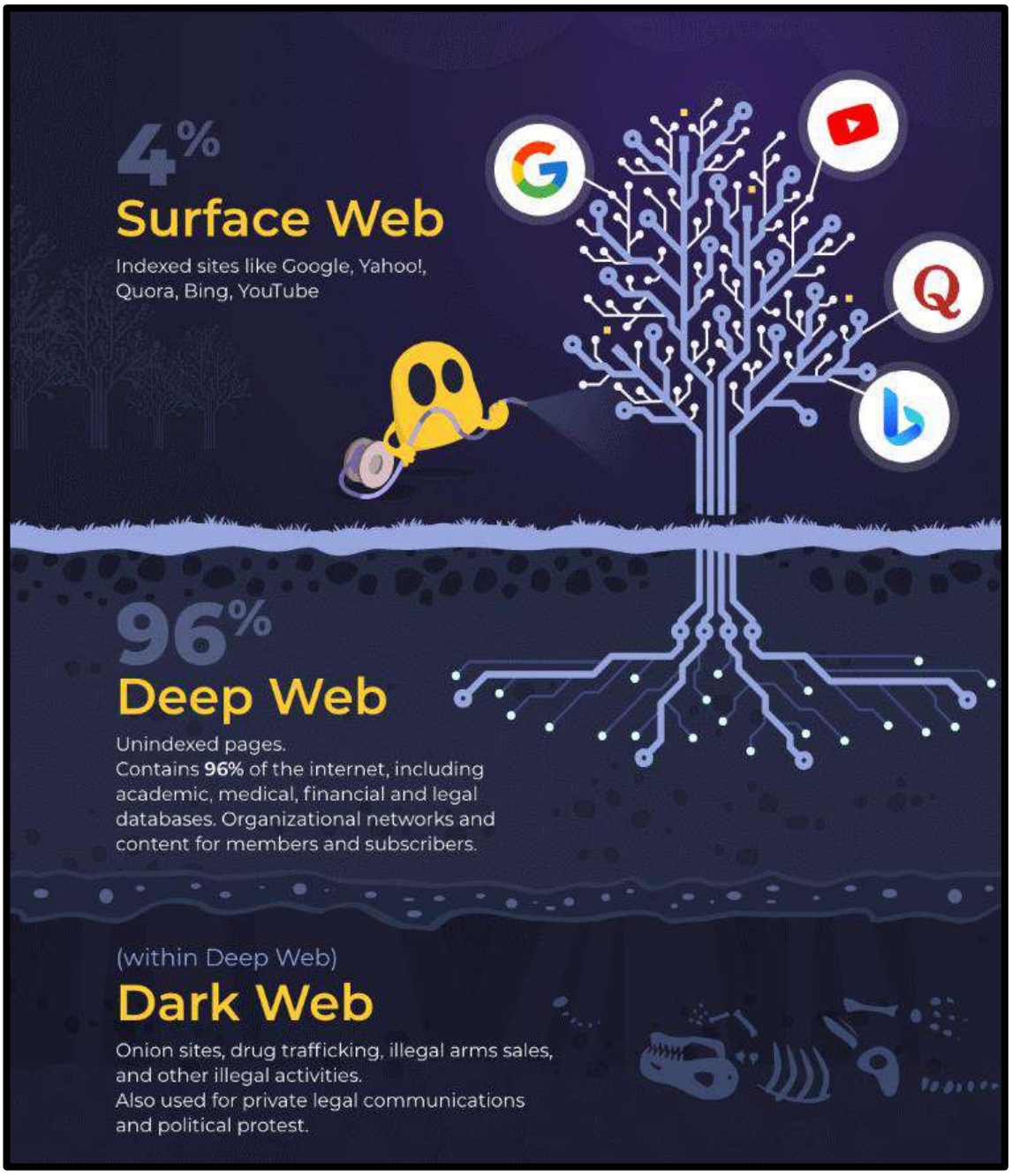


Figure 9:- Intelligence Cycle

4. Dwhere we are operating inClearWEBorDeepWEB?

Before starting our research or information gathering activity, it is good to make a premise about the fields in which an OSINT analyst operates, or to define what is meant by ClearWEB, DeepWEB and DarkWEB.

The**ClearWEB**or**SurfaceWEB,**it's the art of the internet that we're all familiar with and it's the part of the internet that we all access on a daily basis. It includes websites and resources indexed by search engines such as Google, Yandex or Bing. Think of everything you can find through a simple Google search; this represents only a fraction of the entire internet universe, more precisely around 4-10% of the total.



Let's now move on to**DeepWEB,**which is basically anything that isn't indexed by standard search engines. This includes a wide range of content, from academic databases to government documents, hospital records, and even your personal emails. It is important to underline that DeepWEB is not by nature dark or illegal; it is simply not accessible via normal search engines for reasons of*privacy*and safety.

Inside the DeepWEB, we find the**Darknet**(also called DarkWEB), which represents a small portion of DeepWEB. The Darknet is intentionally hidden and accessible only through specialized software, the best known of which is TOR, an acronym for*The Onion Router* . The main feature of TOR is its ability to anonymize user connections, masking the identity and location of those who browse and those who host the services. One of the best known software that we will encounter later to access the TOR network is**TOR Browser**, but also **Well done**which has a module inside that allows navigation.

One of the myths to dispel is that accessing the TOR network is illegal. In reality it is a tool that is mainly used for digital freedom, especially in those countries where there is no freedom of expression. In fact, using this network, activists and journalists are able to communicate securely and freely access different sources. However, the presence of multiple criminal activities such as drug trafficking, sale of weapons, sale of personal data, sale of false documents, production of child pornography films, etc. should not be ignored.

5. USO AND INSTALLATION OF ONEVPN

Let's start by saying what a VPN is, or a Virtual Private Network. It is software that creates secure and encrypted connections between your device (PC or Smartphone, etc.) and a server managed by the VPN provider (e.g. NordVPN). This encrypted tunnel allows us to ensure that the data transmitted is secure and private.

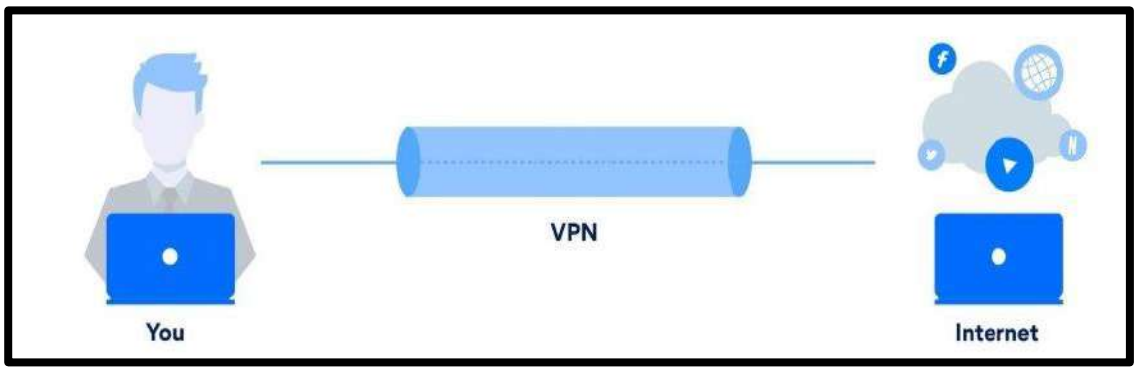


Figure 10:- Example of VPN Connection

This is useful for:

- or protect your personal data while browsing;
- or stem any censorship and restrictions in the geographical area where we are located (for example investigative journalists operating in totalitarian countries);
- or additional security when connecting to public networks.

Having said this, it is easy to understand the reasons why the VPN is one of the fundamental elements during OSINT analysis work. In particular:

- *identity protection*: thanks to the fact that it hides the IP address of the real operator, it manages to protect his identity throughout the collection of information;
- *improve information search ability*: by connecting to a foreign server, we can view and acquire information from a local server (for example, collecting information from a user in Africa, we choose the server that is located in the same country as the target or the adjacent one).

Figure 11:- Example of VPN Software Servers

6. PASSWORDMANAGER

Using a password manager (*Password Manager*) is a practice that can help users securely and efficiently manage their login credentials. In fact, when you create many avatars to which you associate different social profiles and services, it is sometimes impossible to remember all the passwords. This is why it is important to equip ourselves with similar software and a multiplatform that we can use to always have with us in a few moments all the access to the services and avatars we have.

Password managers are tools that store and organize passwords and other sensitive data, encrypting them in a digital "safe" protected by a unique master password.

7. CREACTION OF ONEWORKSTATION

Once we have defined which environment we are operating in, it is important to create our working environment.

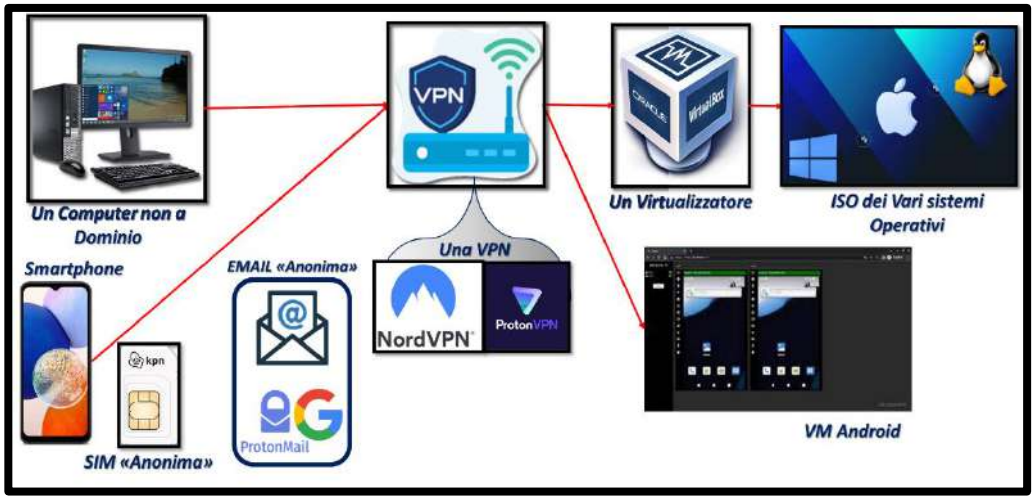
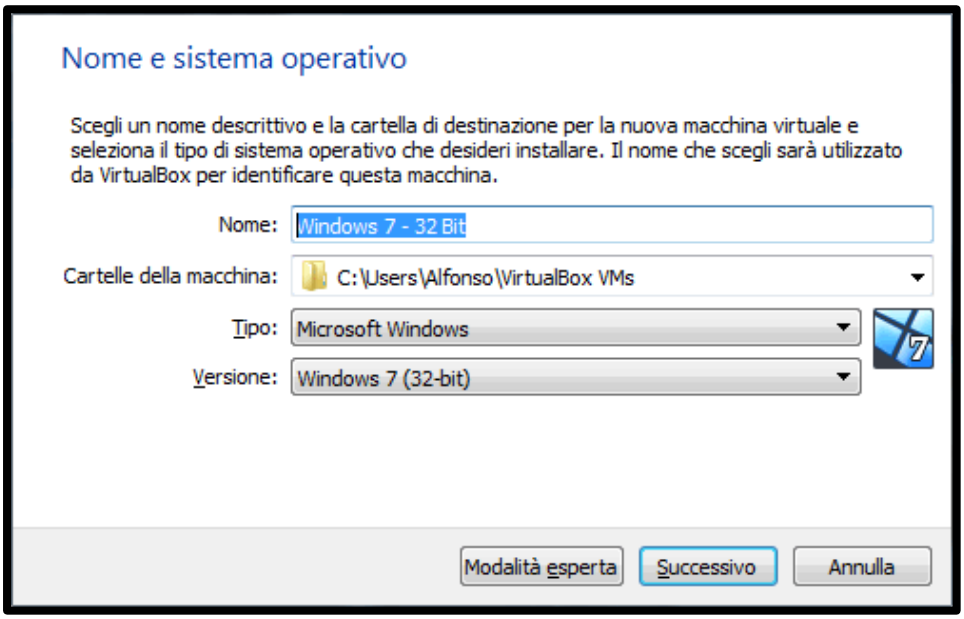


Figure 12:- Creation of a Workstation for OSINT

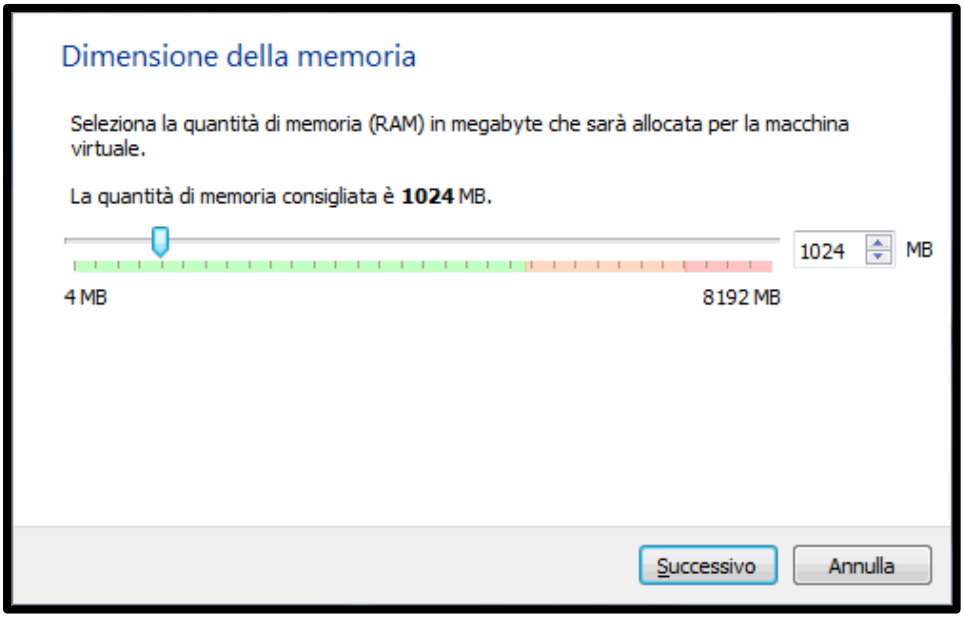
Creating a Workstation specifically configured for OSINT activity requires attention to various technological and security aspects. We start with a computer without an institutional domain and finally install virtualization software such as VMware or VirtualBox.

Below we will indicate the steps for creating our Virtual machine with the VirtualBox software. After downloading and installing via the site *https://www.virtualbox.org/wiki/Downloads*the most updated version of VirtualBox and the Extension Pack, we proceed to install our virtual machine.

1. Click on New.

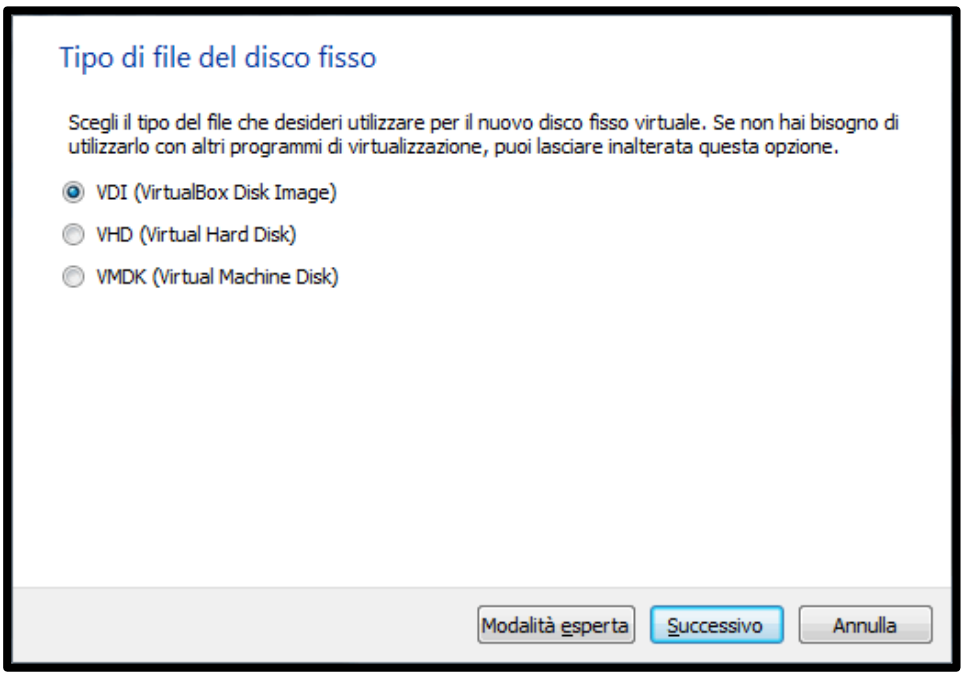


2. Enter a name of the operating system we want to configure. We choose in which folder to insert all the files that will make up our VM (Virtual Machine), choose what type of VM you want to initialize (Windows, Linux or Mac) and the version.

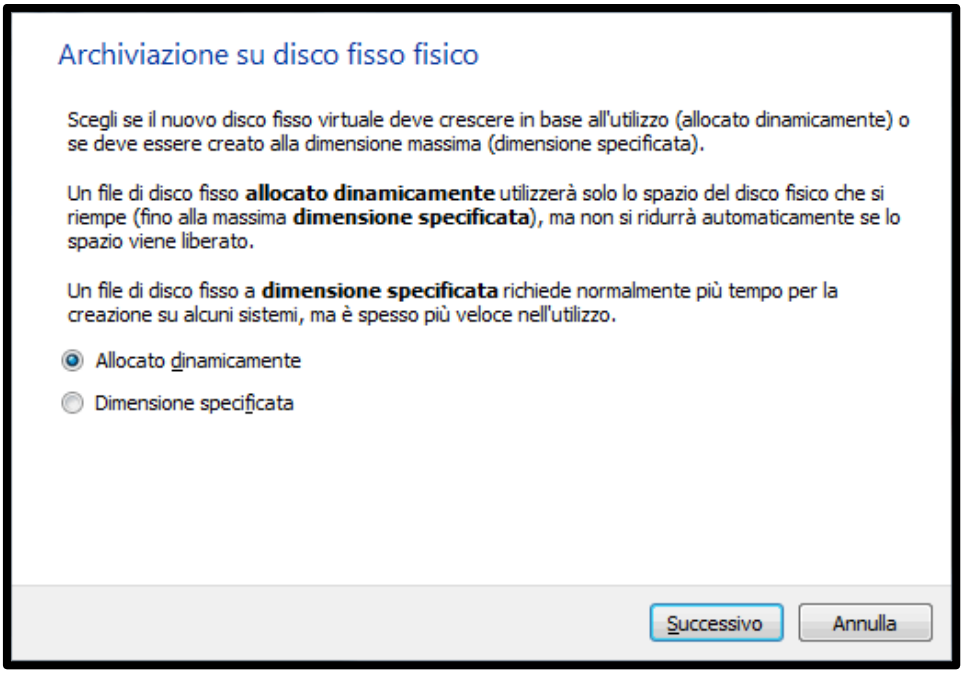


3. Choose the amount of RAM needed to work on our VM.

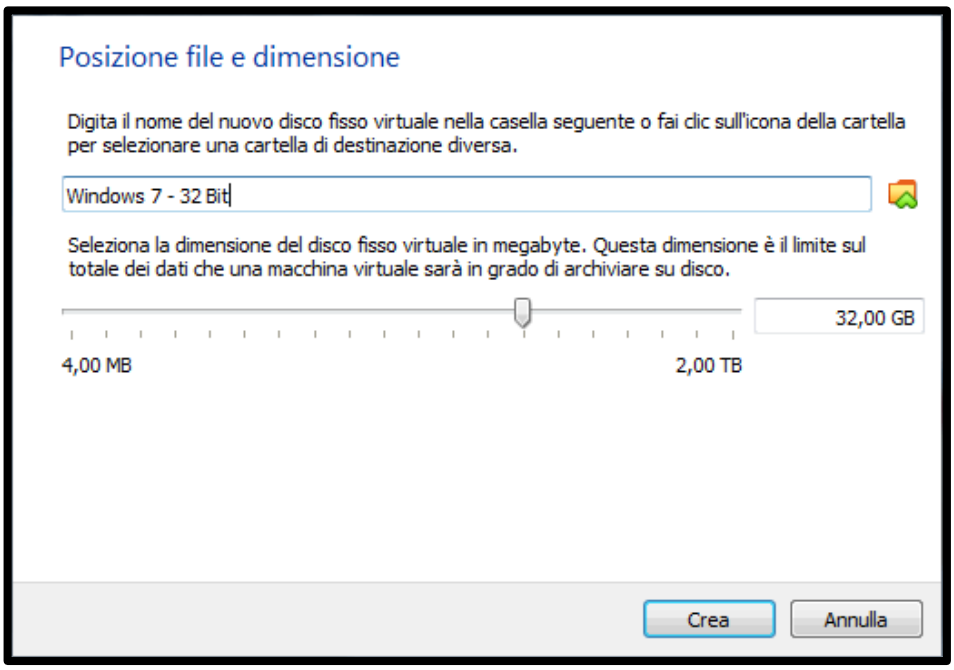
4. We can insert an already existing virtual disk, or create a new one.



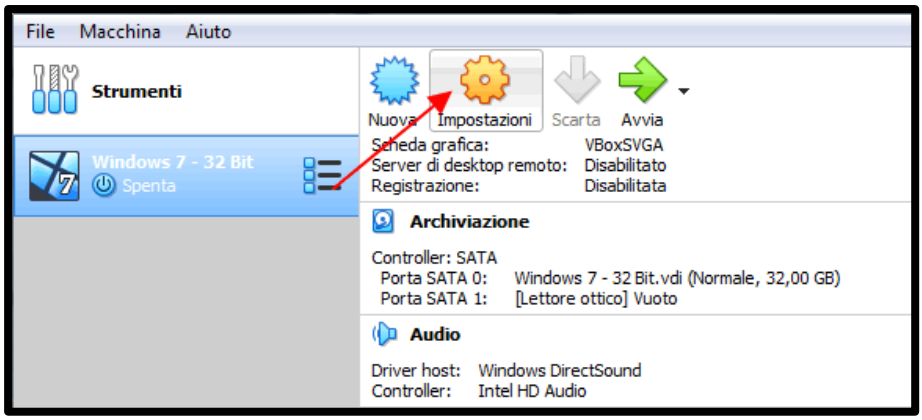
5. Choose the extension of the disk we want to create. This can be important if we then want to use our VM on another platform or another computer that has virtualization software installed such as VMware or Hyper-V.



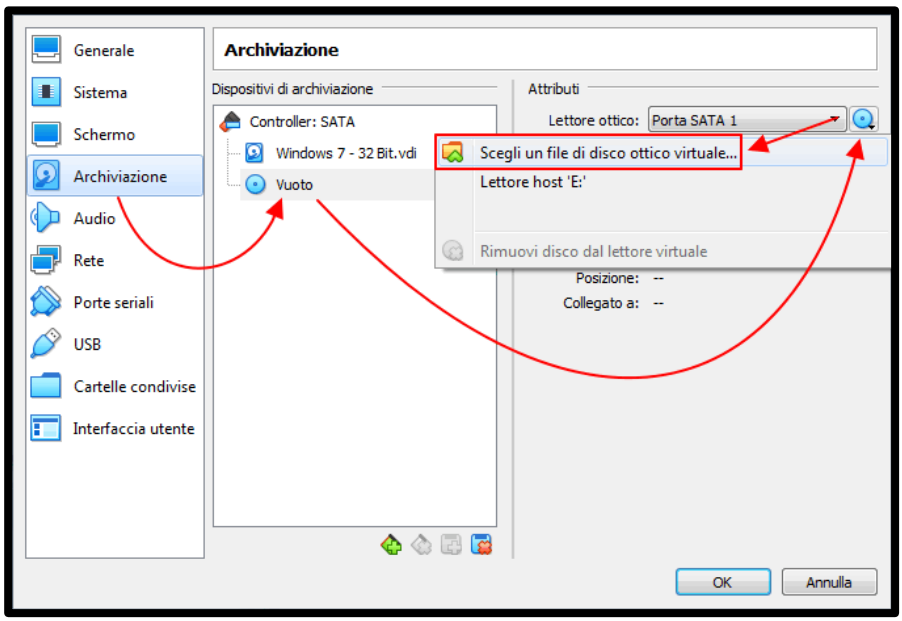
6. Choose the type of storage on the hard disk, whether dynamic or with maximum storage.

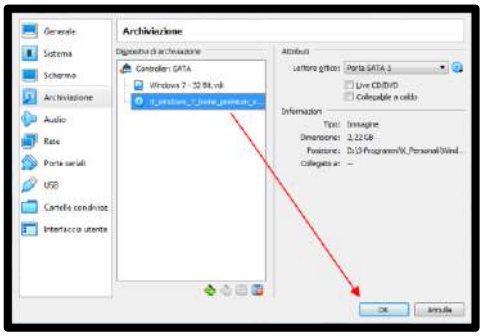


7. Choose where to store the disk and its size and press Create.

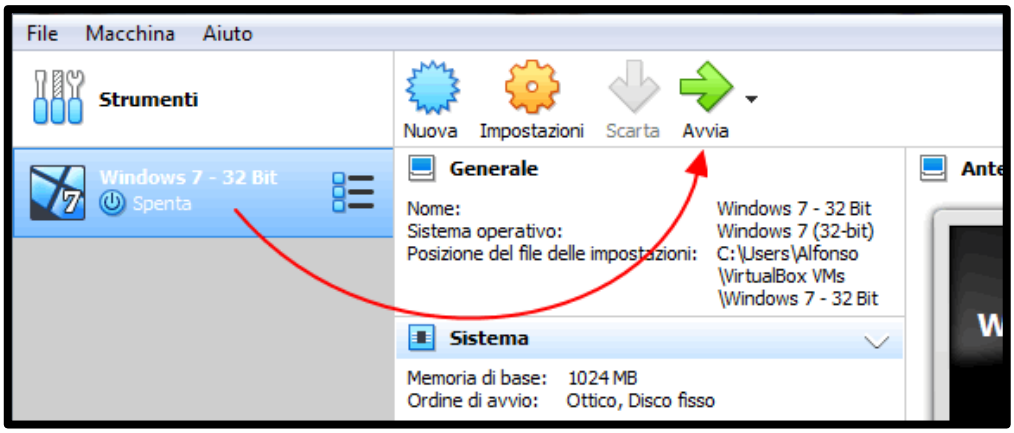


8. Once we have created our virtual machine, we need to put our operating system inside. Once we have selected our virtual machine, we go to Settings.





9. We go to "Storage", click on the empty disk and then click "choose a virtual optical disk file...", then we go to the folder that contains our .iso and load it and finally press "ok".



10. Now we can start our virtual machine either with a double click or by pressing the Start button.

8. ISOANDDISTROLINUXWINDOWS EMB.C

Once we understand how to create a virtual machine, we need to understand what type of image we want to use for our business.

There are different types of images depending on the working mode and setting of our VM. Let's start with the most common ones which are:

- **Kali Linux**-*https://www.kali.org/get-kali/*
- **Tsurugi Linux (see 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*

Figure 13:- Virtual Machine Linux

Subsequently, there are VMs already configured with all the tools we need for our OSINT activity, such as:

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

9.BROWSER EMOTORI DIRSEARCH

The use of browsers dedicated or configured specifically for Open Source Intelligence (OSINT) activity is essential to guarantee security, anonymity and effectiveness during the collection of information and beyond. As we will see, some of these software were created precisely to guarantee maximum performance*privacy*to the user, while others can be configured specifically. Below we will see three of the main browsers that are used for browsing the internet.

9.1. TorBrowser

Tor Browser is based on Mozilla Firefox and is designed to anonymize user traffic using the Tor network which we have already covered in previous chapters. This process, known as "onion" routing, encrypts data multiple times and passes it through multiple nodes, removing a layer of encryption at each step. This path pays off extremely difficult to trace the origin of traffic, guaranteeing user anonymity. This browser is particularly useful for OSINT analysts who need to hide their IP address and geographic location to access information protected by geo-restrictions or to safeguard their identity.

Among its characteristics we therefore have:

- **Anonymity:**Tor Browser masks the user's IP address, making it almost impossible for websites, advertisers and any external observers to identify the true origin of the traffic;
- **Access to websites. onion:**the Tor network hosts special websites with the ".onion" extension, which are not accessible via traditional browsers. These sites offer additional levels of*privacy*and anonymity;
- **Protection against tracking**: Tor Browser is configured to block trackers and tracking attempts*fingerprinting*browser, which tries to identify users through their device configurations;
- **Default security:**the browser offers different levels of security that users can adjust depending on their needs. These settings affect things like JavaScript execution, fonts, and other components that can be used to track users.

Installation and Settings*privacy*

Being multiplatform, TOR can be installed via:

- links -*https://www.torproject.org/*
- command line through the Linux terminal:

or *Sudo add-apt repository-y ppa:micahflee/ppa*

or *Sudo apt-y update*

or *Sudo apt install-y torbrowser-laucher*

- Google Play store and Apple App Store.

9.2. MozillaFireFox

Firefox is highly customizable and can be configured with various extensions and settings to improve security and*privacy*. It is one of the most popular and respected web browsers, known for its flexibility, robust features*privacy*and for his open philosophy of development. It is created and distributed by*Mozilla Foundation*, a nonprofit organization dedicated to promoting an open and accessible internet.

Among its advantages we have:

- **private browsing mode**: prevents saving of browsing history and cookies;
- **improved tracking protection:**Firefox automatically blocks many third-party trackers, including incognito content tracking and cross-site cookies;

- **private browsing mode:**Similar to other browsers, Firefox's private mode does not save browsing history or cookies;
- **protections against fingerprinting:**Firefox includes protections against advanced fingerprinting techniques that attempt to identify users based on their device configurations.

Installation and Settings*privacy*

Since it is also multiplatform, we can install the browser via:

- website:*https://www.mozilla.org/en-US/firefox/new/*
- Linux terminal command line: or

  Sudo snap install firefox
- Google Play store and Apple App Store.

Furthermore, there are two methods, a basic one and an advanced one, to increase security and safety*privacy*of the browser.

- **Basic Configuration:**through the Menu - Options - item*Privacy*And Security, we can:
  - activate “Clear cookies and site data when Firefox is closed”;
  - enable “Notify me when websites try to install add-ons”.

- **Advanced Configuration**
  - insert**about:config**in the address bar and proceed to “show all”.
  - proceed with the following configurations:

set on**False**:	set on**True**:
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

The Brave browser has become popular for its focus on*privacy* and online security. It is built on the same engine as*Chromium*[2], which also powers Google Chrome, but stands out with a few key Chrome-oriented features*privacy*.

Among its main features we have:

- **ad and tracker blocking:**Brave automatically blocks ads and trackers while browsing. This not only speeds up browsing but also protects users from tracking*cross-site.*This means that while browsing you can view and analyze sites without significantly changing your digital profile or leaving traces.
- **advanced protection against fingerprinting:**Fingerprinting is a technique used to uniquely identify visitors to a website through the combination of various information from their device. Brave offers advanced protections against fingerprinting, so you can minimize your visibility.
- **Built-in Tor:**Brave includes the ability to open a private tab with Tor, which offers an additional layer of*privacy*hiding the IP address and encrypting web traffic through the Tor network.
- **HTTPS Everywhere:**Well done integrates"*HTTPS Everywhere*", which forces connection to websites via HTTPS when available, ensuring an encrypted and more secure connection.
- **integrated cryptocurrency wallet:**also offers a*wallet*integrated for cryptocurrencies, which could be useful for those involved in investigations relating to blockchain or cryptocurrency transactions.

Installation and Settings*privacy*

The Brave Browser can be installed:

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

[2]Chromium is a free and open-source web browser project, primarily developed and maintained by Google. It is a widely used codebase, providing the vast majority of code for Google Chrome and many other browsers, including Microsoft Edge, Samsung Internet, and Opera. The code is also used by several app frameworks.

- Linux command line or

  sudo apt install curl

  or *sudo curl -fsSLo /usr/share/keyrings/brave-browserarchive-keyring.gpg*

  or *https://brave-browser-apt-release.s3.brave.com/ bravebrowser-archive-keyring.gpg*

  or *echo "deb [signed-by=/usr/share/keyrings/brave-browserarchive keyring.gpg] https://brave-browser-aptrelease.s3.brave.com/ stable main"|sudo tee /etc/apt/sources.list.d/brave-browser-release.list*

  or *sudo apt update*

  or *sudo apt install brave-browser*

9.4. MOTORI DIRSEARCH

Although Google is a very powerful and efficient search engine, it is not the only option we have, in fact there are other search engines that allow us to explore various data that Google does not show us for various reasons and which can allow us to narrow the field on what our research is.

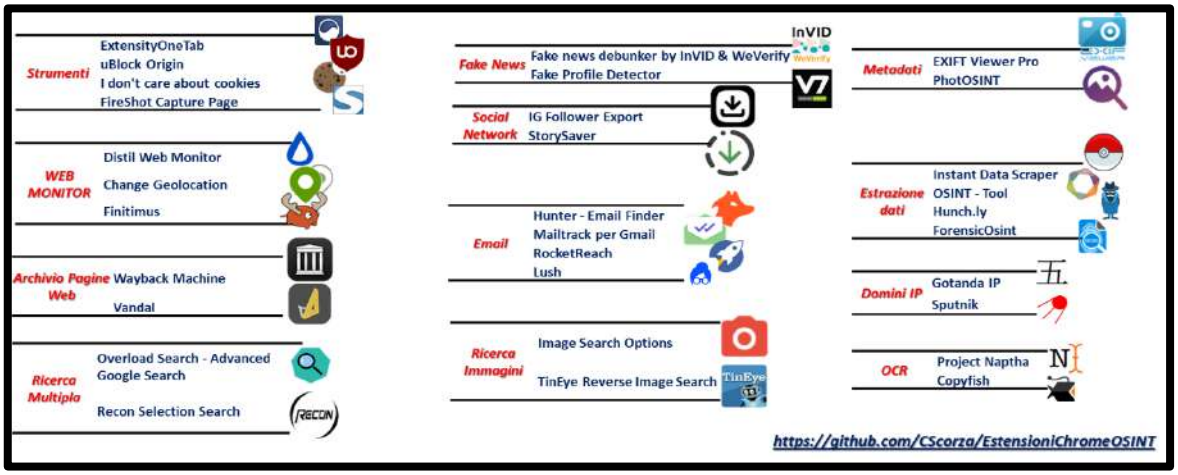
Among these search engines we have:

- ***DuckDuckGo****(https://duckduckgo.com/)*, *great for user privacy, but also because it uses a country-specific search operator. It also allows you to search on .onion sites*
- ***Yandex (****https://yandex.com****)****oriented for searches in Russia and Eastern Europe, it is very efficient for Reverse Image (image search) and the translation of texts present in images.*
- ***Baidu (****https://baidu.com****)****it is one of the most used search engines in Asia Eastern (particularly in China), it is in fact a search engine that indexes many sites present in that geographical area.*

- ***Onionengine (****https://onionengine.com****)****it is one of the many search engines for .onion sites, therefore all those services that are on the Tor network.*

9.4.1. BROWSER EXTENSIONS

In addition to the browser and search engine, there are additional tools that can be used for our data collection. These tools are called "Extensions –*add-ons*" and are usually present in all the most popular browsers such as FireFox, Brave and Google Chrome. They integrate with internet browsing software and help us collect and analyze the web pages we are browsing and more. Obviously, it is highly recommended, except in exceptional cases, to download and install these tools, only from the official source.



For OSINT activity there are many famous and less famous ones. Below are some that may help.

Tools for anonymity and privacy control	***UBlock Origin***	***NoScript***
	Ghostery - Ad Blocker for Privacy	***I don't care about cookies***
Screen Capture - Scraping	***ForensicOsint***	***Nimbus Screenshots***
	Go Full Page	***FireShot Capture Page***
	Hunch.ly	***OSINT - Tool***
	Tinking - Scrapping Tool	***Instant Data Scraper***
Web Monitor	***Change Geolocation***	***Finitimus***
Metadata	***EXIFT Viewer Pro***	***PhotoOSINT***
Deepfakes	***Fake news debunker***	***Fake Profile Detector***
Multi Search	***Overload Search***	***Recon***
	Selection Searc	
Web Pages archive	**Wayback Machine**	***Web recorder ArchiveWeb.page***
	Vandal	

Image Search	***Image Search Options***	**RevEye Reverse Image Search**
	TinEye Reverse Image Search	**Download All Image**
Email analysis	***Hunter - Email Finder Extension***	**Mailtrack for Gmail: Email tracking**
Email Search on Social Media	*RocketReach*	***SignalHire***
Social Networks	***IG Follower Export too***	**Story Saver**
	Treeverse (Twitter)	
Domain Analysis	***Gotanda***	***IP Address and Domain Information***
	Sputnik	

Figure 14:- Useful extensions for the Browser

10. SOCMINT - SOCIALMEDIATHENTELLIGENCE

Social Media Intelligence is a branch of intelligence that focuses on the collection and analysis of information available on social media for various purposes, certainly including intelligence gathering or strategic information.

This branch of OSINT exploits the data left by users, their online behaviors and the various interactions between various users on social networks such as Facebook, Instagram, Twitter, Linkedin etc.

The main activities of SOCMINT are:

- **Content analysis**: which includes the analysis of posts, comments, images and videos published by users on social media. This allows you to understand the opinions, feelings and trends that can emerge from the amount of data generated by users.
- **Network analysis:**the analyst in this phase explores social networks to identify connections between users, such as friendship networks, mutual influences, etc.

- **Geolocation:**Many posts on various social media sites include geolocation data, which can be used to determine where users were at the time of posting.

Obviously all this data needs further verification and analysis, as it is data entered by the user and therefore easily falsified.

10.1. CREACTION OF ATOVATAR(SOCKPUPPET)

One of the fundamental pillars for every OSINT analyst is to create different avatars or sockpuppets (i.e. fictitious entities), used to collect information without therefore revealing the operator's true identity. The use of avatars is essential to access various information in various online environments. Let's think about forums on the Darknet or certain social networks that point out the view of their profile to the user being analysed. Furthermore, it is

Its creation is also fundamental in order to make it as credible as possible in the environment we are exploring. For this reason, below we will see the various steps that can help us in creating our identity, from the creation of a credible biography, to the choice of the profile picture, to the use of a SIM not registered in the name of the choice of a secure email .

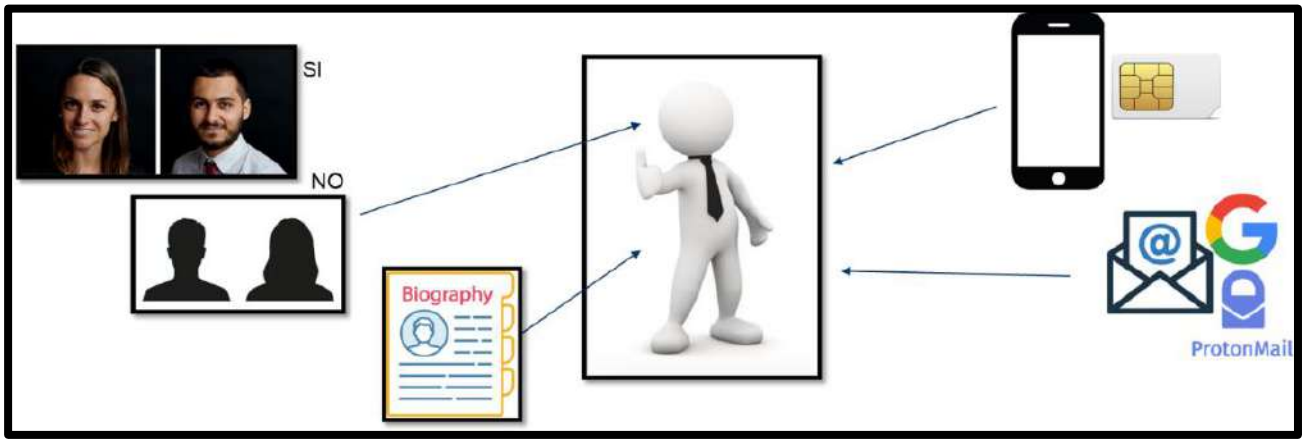


Figure 15:- Elements for creating an AVATAR

10.2. BIOGRAPHY

Creating a compelling bio for an avatar requires attention to detail and an understanding of the context in which the avatar will operate and therefore its use.

So one of the questions you need to ask yourself when creating your biography is:

- What is the objective of the operation? (collection of information or monitoring of a specific target);
- In which environment will it operate? (Dark WEB, Social Networks and the content in which it will move);
- In what context? (religious, political terrorism, hacker groups, child pornography etc.).

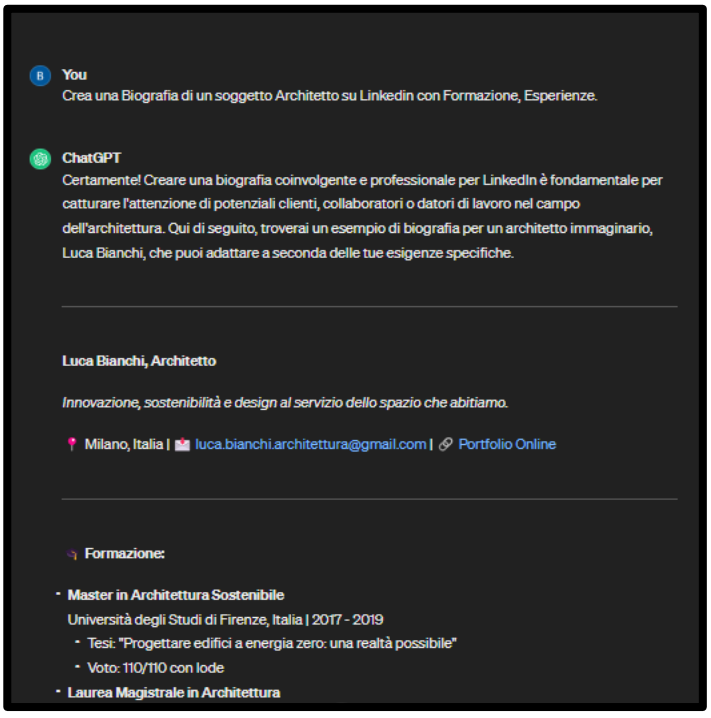


Figure 16:- Creating a Bio with GPT Chat

For this reason it is necessary to develop a *background*" personal information that includes not only the name and surname, but also a consistent chronological age, place of residence/birth, education, career and occupation as well as hobbies and various interests. It goes without saying that the choice to enter this information always varies based on the context in which we want to operate. Indeed, there will be gods contexts where the information to be inserted is minimal so as not to arouse particular suspicion, or richer contexts so as not to run risks if there was feedback from our target or even from the social network itself which could ban us for suspicious operations.

Among the various tools we can use there are certainly:

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

10.3. THEIMAGE OFPROFILO

After creating the biography of our avatar, we need to find a profile image to insert on the social network. For this reason it is important to consider various factors, including the credibility of the image and that it is appropriate to the context in which we are operating. In fact, it is important not to use images of real people and perhaps opt for generic images such as those of logos or landscapes, paintings of art or symbols. But many times it is necessary to have images of people, for example from the policies of the social group where we are joining or from the policies of the social network. For this problem we can use different solutions such as:

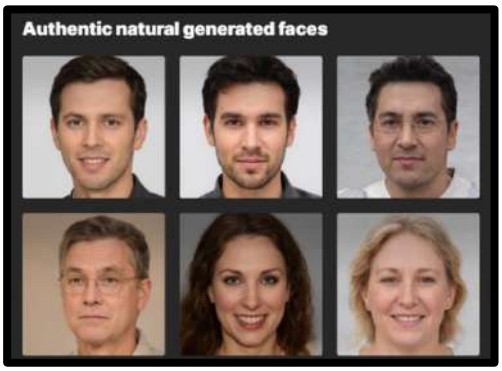


Figure 17:- Authentic natural Generated.photos/faces

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

These tools, like others, allow us to create images of fake faces created thanks to generative networks (GANs) and allow us to modify the face as we like so that we can insert it both in the context of the biography we have created (think of age, ethnicity, etc. .) and in the context where the avatar will operate.

10.4. AND-EMAIL

After creating the bio and avatar, we move on to creating social network signup tools, such as email and phone number. Among the tools we will see are:

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

Starting from email, the most used service for its reliability and security is certainly **ProtonMail**. This is because it uses end-to-end encryption, so that only you and the recipient can access the contents of the emails you send. Also not

it stores log files and allows you to create different email aliases linked to the parent one, in order to manage different entities.

In addition to ProtonMail, Google email (Gmail) can certainly be useful for accrediting ourselves to a social network. This is because the social media subscription policies do not allow the use of ProtonMail.

Figure 18:- Pronton Mail

Another tool is**Simple Login**.

This tool allows you to generate email aliases that forward messages to your primary email inbox. These aliases can be customized, deactivated or deleted at any time and this allows us complete and flexible control over all our entities.

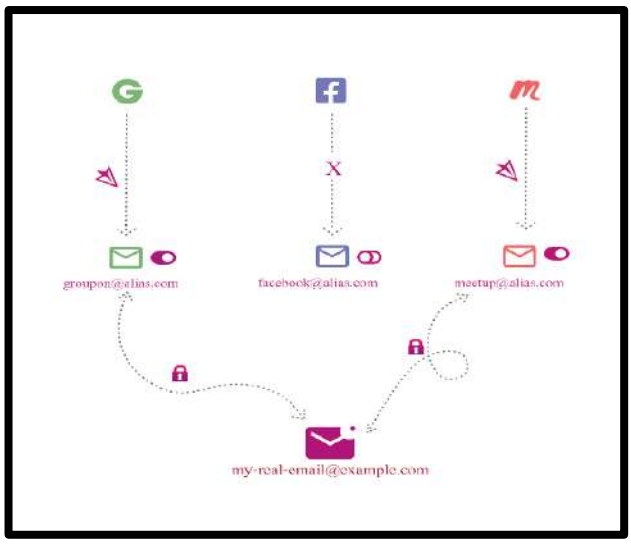


Figure 19:- Simple Login.

10.5. NOUMER OFTELEPHONE

In many cases, when registering on a social network or creating an email, a telephone number is required to authenticate the profile. Obviously for several reasons the use of your personal number is not recommended. For this reason, there are various methods for entering temporary telephone numbers that are not directly traceable to the analyst.

These services are:

- **SMS reception services**
    - *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/*

- **eSIM services**
  - *https://www.airalo.com/it*
  - *https://voice.google.com/u/0/about*
- **Foreign physical SIMs**

10.6. UI KNOW GODSSOCIALNOETWORK FOR THESOCIMINT

One of the main sources of information search are the*Social Networks.*In fact, it represents a powerful tool for collecting, analyzing and monitoring information relating to people, organizations and events of interest.

The first step, once we have identified the social networks frequented by our target, consists in registering a fictitious profile (sockpuppet/avatar). This allows us, if possible, to access profile pages and collect data that would otherwise not be visible.

Below we see which are the most popular social networks and which tools to use for our OSINT activity.

10.6.1. FACEBOOK

Facebook is one of the most famous META social networks and thanks also to the vast diffusion it has had over the years, it is an enormous source for the analyst due to the quantity of information and data that can be obtained. In fact, through the profiles of our targets it is possible to obtain a lot of information such as:

- ***the ID*** *:that is, a unique identifier assigned to each user account;*
- ***Personal data*** *:name and surname, date and place of birth and place where you live;*
- ***Contacts*** *:telephone numbers and emails;*
- ***Networks of friends and relatives*** *:it is possible to identify which users are the most active and any family ties;*
- ***Hobbies and personal information*** *:through the posts and information entered by each individual user it is possible to derive a whole series of interests;*
- ***Geolocation of images and videos*** *:with the geolocation that the user inserts into the images but also from the context that represents the image itself it is possible to know in which place it was taken;*
- ***The "Tags" of the photos*** *: with Tags we can also know the names of the people "tagged" in the photos and videos.*

TOOLS FACEBOOK

The tools used for analyzing Facebook profiles are:

- **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-datascraper/ofaokhiedipichpaobibbnahnkdoiiah

- ***Dumpitblue+***

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

- ***FBDOWN.net***

  https://fdown.net/

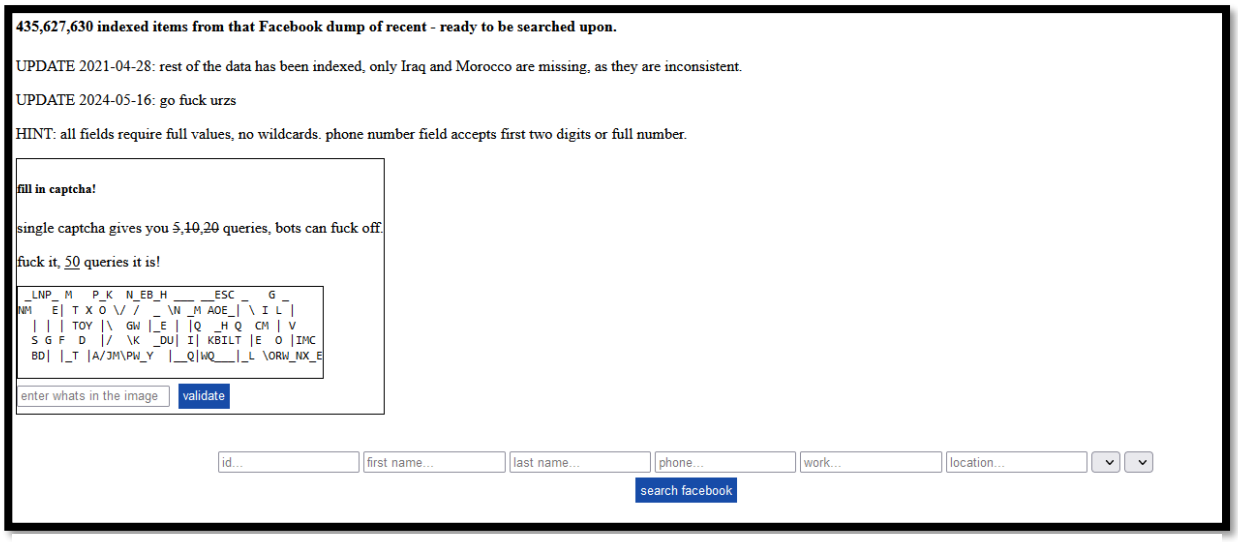


Figure 20:- Fuck Facebook

10.6.2. THENSTAGRAM

The second META social network that we can use for research and collection of information is Instagram.

However, it is not as simple as Facebook to obtain the information, this is because of the restrictions of*privacy*used by users are greater.

However, as with Facebook, among the information we can obtain is:

- *Nickname and first and last name of the user;*
- *Personal data if indicated;*
- *Contacts (via reactions to photos or looking at followers and following);*
- *Networks of friends and possible relatives;*
- *Information such as hobbies and travel;*
- *Geolocation of photos both via user setting and image context;*
- *The various tags of other profiles in your photos.*

TOOLS INSTAGRAM

Among the various tools that we can use and currently working we have:

- ***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-disistenza/kicgclkbiilobmccmmidfghnijgfamdb
- ***IG Email Scraper*** *https://chromewebstore.google.com/detail/ig-email-scraperextracto/cmlfhilehabkgmicijgaonjgdkiclcna*

- ***Instaloader***

  https://instaloader.github.io

10.6.3. LINKEDIN

This social platform is mainly used by professionals in each sector for job search but also by the professional network of each sector. This goes without saying that this social network has enormous potential in terms of data both for searching for members of an organization and for personal information linked to the individual user.

Before starting to see what data can be extrapolated from the single target, let's first see how we can set up our profile*fake*in mode*stealth.*This is because social media, by its nature, tends to make users interact in order to create professional networks. But our purpose is to monitor and collect information, without the user being aware of it. Below are the different steps for setting up your profile:

- Let's go to the top icon “YOU”
- Settings e*privacy*
- Visibility

- And let's change the settings of both the "**visibility of your profile and network**" that of the "**visibility of your business on Linkedin**" as shown in the two attached photos (Figure 13)

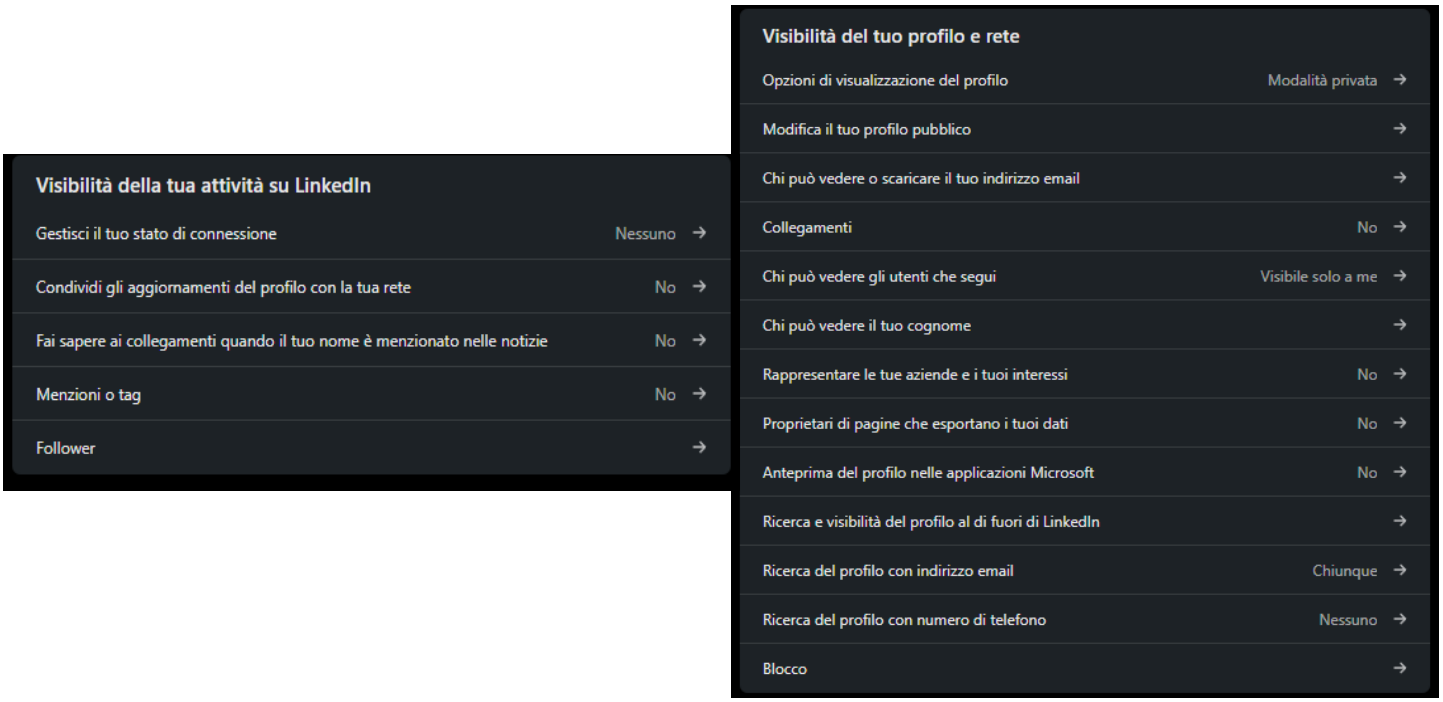


Figure 21:- LinkedIn profile privacy setting

Once we have set up our profile, we move on to collecting the information we can find on the various LinkedIn profiles. Among the various information we have:

- Nikname in the "Urls";
- Name and surname;
- Profile picture;
- Profession and work experience;
- Biography;
- Profile creation date;
- Number of followers and followings;
- Posts and activities published.

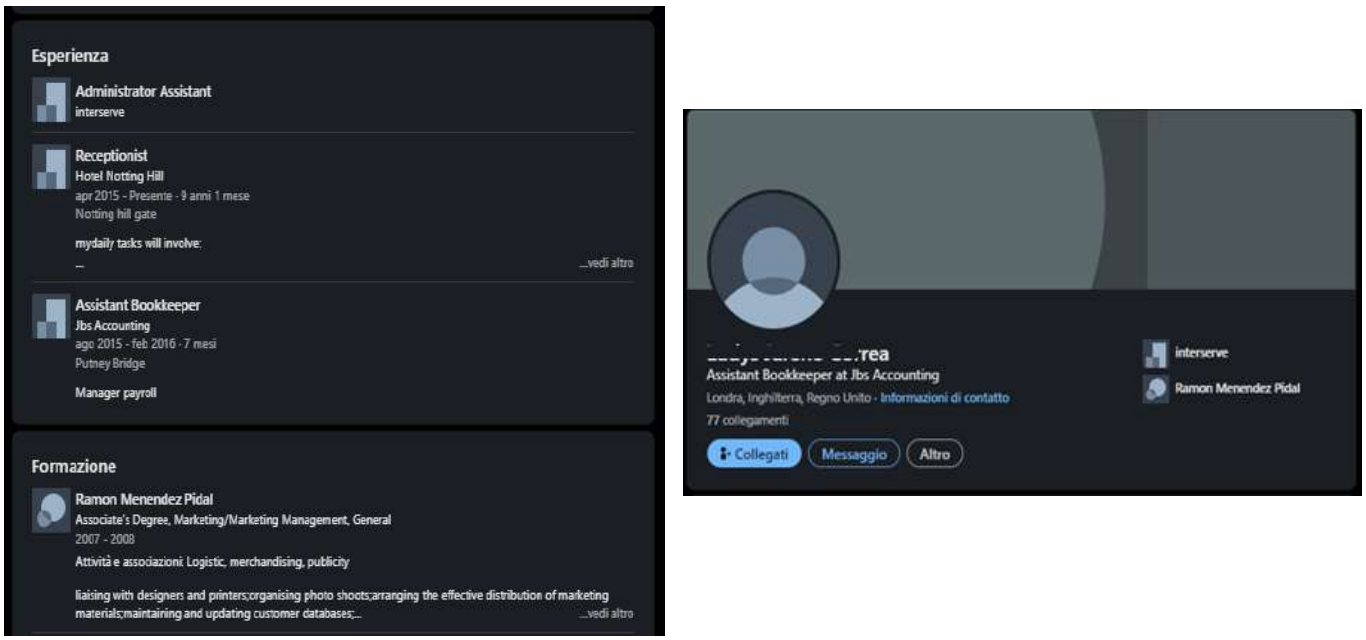


Figure 22:- Public information within the LinkedIn profile

If we want to search for the members of an entire organization, we can use the search bar and set the various filters to optimize the search. In this way, as a result we would have all users who, among their information entered in their profiles, include the name of the organization that we have entered as work experience or current work.

In the attached example (Figure 15), we searched for all users who work or have worked for ENI SpA

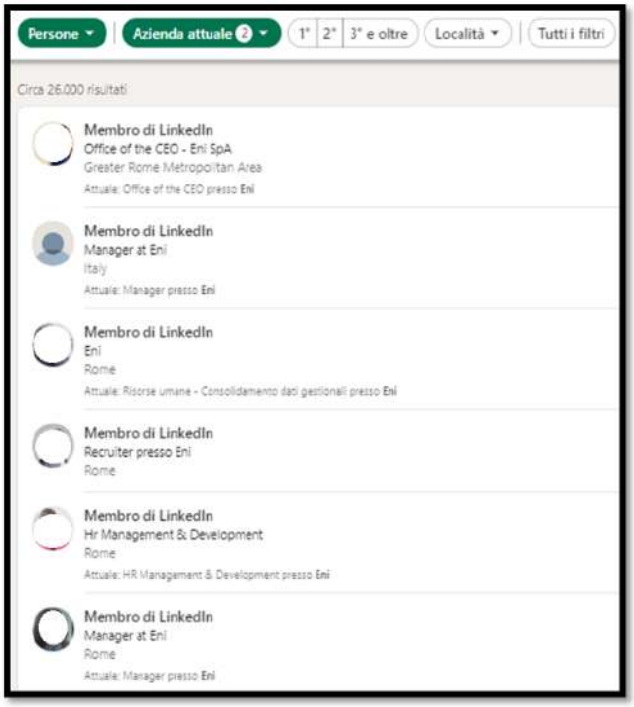


Figure 23:- Example of search for ENI SpA members

TOOLS LINKEDIN

Among the various tools we can use on LinkedIn there is:

- ***Expertsphp***

  https://www.expertsphp.com/linkedin-video-downloader/

- ***RocketReach***

  https://chromewebstore.google.com/detail/rocketreach-chromeextens/oiecklaabeielolbliiddlbokpfnmhba

- ***SignalHire***

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

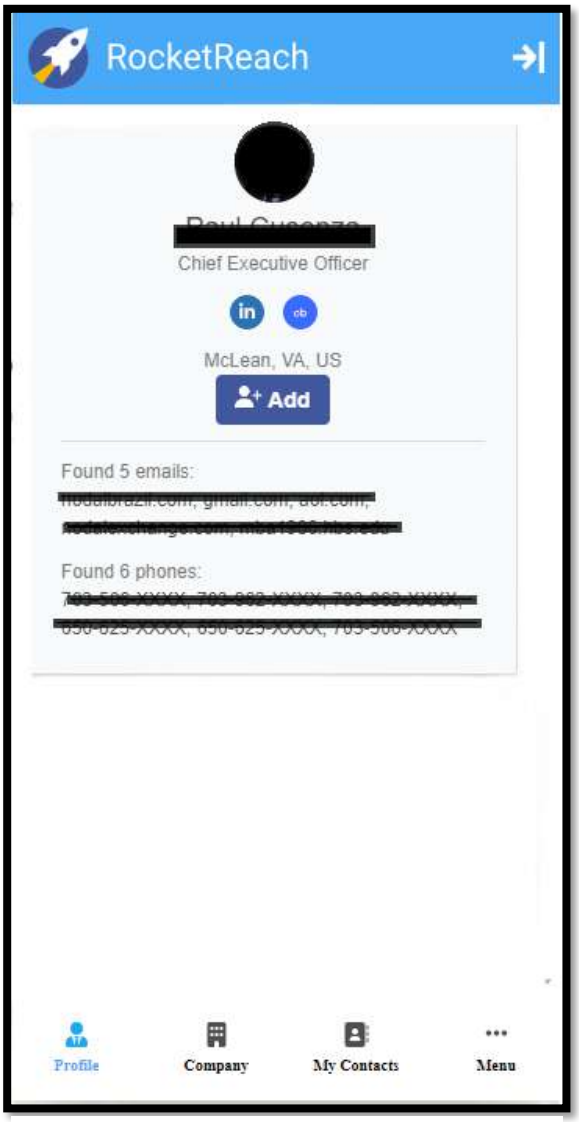


Figure 24:RocketReach

10.6.4. TWITTER/X

Twitter, today "X" after the acquisition of Elon Musk in April 2022. It is a socia
widely used by users to express opinions, follow trends, etc. Thanks to this it
many analyzes and information gathering. In particular, it is possible to mon
of a topic thanks to users' use of hashtags in their tweets. Furthermore, usin
be listed later, it is also possible to establish a geolocation of the "*trend*" or u
personality of a profile etc. Obviously through advanced search and the use of various filters, it is possible to improve the search for individual posts or user profiles.

When examining the user profile we can obtain the following information:

- *Analysis of the username (which can also correspond to a nickname used in another social profile or forum);*
- *Biography if present;*
- *Check profile creation date;*
- *Number of followings and followers;*
- *Reading tweets, including historical ones, also noting any links to other websites or social networks and related hashtags;*
- *Finally, profile photo and background photo, then OSINT Image.*

Figure 25:- Twiiter/X

TOOLS TWITTER/X

Among the tools that we can use on Twitter mainly for monitoring and analyzing tweets, we have:

- ***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/*

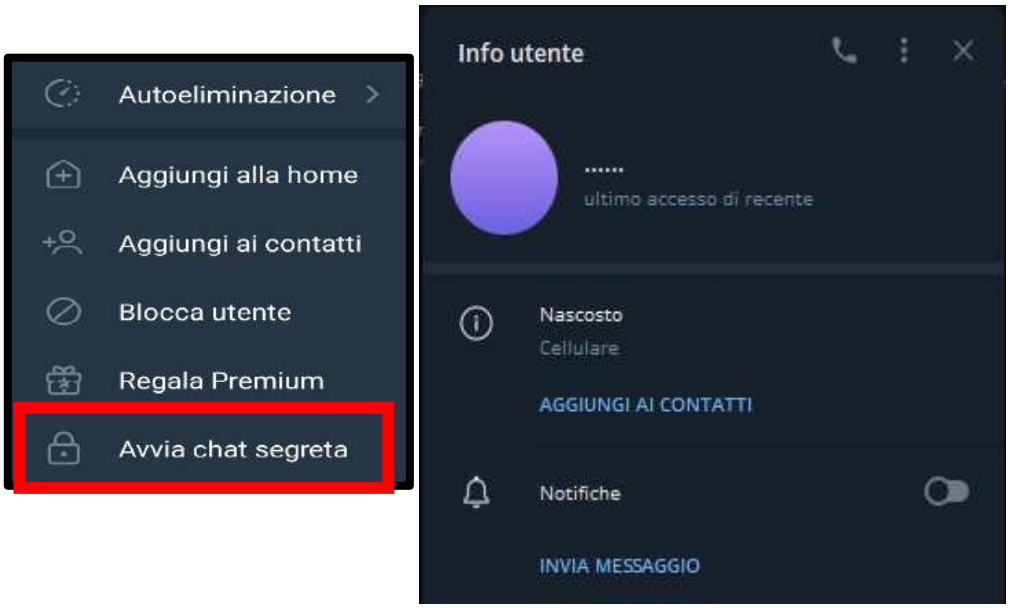
10.6.5. TELEGRAM

Telegram is a messaging app used and popular all over the world for its robust messaging options*privacy*and safety. In fact, it is used by many criminal organizations of various types, for the exchange of data and more.

- Among the characteristics of individual users we have:
    - Profile photo;
    - Nickname;
    - Biography.

However, this information can be omitted by the individual user, making it difficult for the OSINT operator to search for information. In fact, it is possible to find profiles that do not release any useful information for recognition.

- Among the main features of the messaging platform we have:
- **Secret chats with end-to-end encryption:**some chats can be set up in a cryptographic way so that the conversations are visible only on certain devices and therefore by the users who are members of the chat.



- **Public and private channels and groups**: Users can create and/or join various public and private channels and groups. The difference lies in the fact that the channels are used for the dissemination of news and content and there is a dialogue with the members. In the group, however, we have the exchange of messages and data between the members.
- **Telegram BOT**: Allows developers and administrators of groups and channels to perform and automate the management of tasks and services within groups and beyond.

- **Developer API:**Telegram APIs therefore allow you to create these applications and services that interact directly with the platform.

Below we will indicate the Web services that give us support for the search and analysis of Telegram groups and the most used BOTs for the search, analysis and monitoring of Telegram groups and profiles.

Figure 26:- BotFather

TOOLS Telegram

Among the tools we can use to search for groups and channels and monitor information we have:

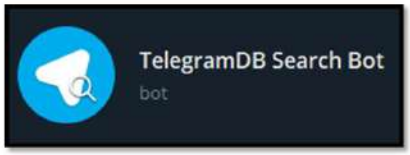
Figure 27:- Telemetryapp.io

- ***Telemetryapp -****https://www.telemetryapp.io*
- ***Telegram Search Engine -****https://xtea.io/*
- ***Telegram Group -****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*

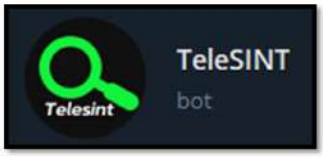
In addition to these tools, there are, as we mentioned before, BOTs. Of these we highlight some that can be of support during the collection and analysis phase of Telegram profiles and channels.

- *https://t.me/maigret_s2_bot* (***Username search***)
- *https://t.me/tgdb_bot* (***Search for related groups***)
- *https://t.me/telesint_bot* (***Telegram ID Search***)
- *https://t.me/Quick_OSINTbot* (***Search for profile information***)
- *https://t.me/holehe_s_bot* (***Search email info***)
- *https://t.me/ooSearchBot* (***Search for groups, channels and BOTs***)
- *https://t.me/TrueCaller_Z_Bot* (***Search name by number telephone***)

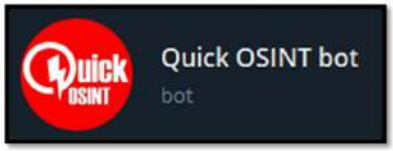
https://t.me/maigret_s2_bot



https://t.me/tgdb_bot

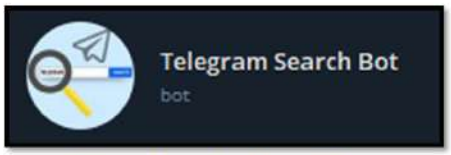


https://t.me/telesint_bot



https://t.me/Quick_OSINTbot

https://t.me/holehe_s_bot



https://t.me/ooSearchBot

11. AANALYSIS OFUSERNAME/NOROYAL HOME

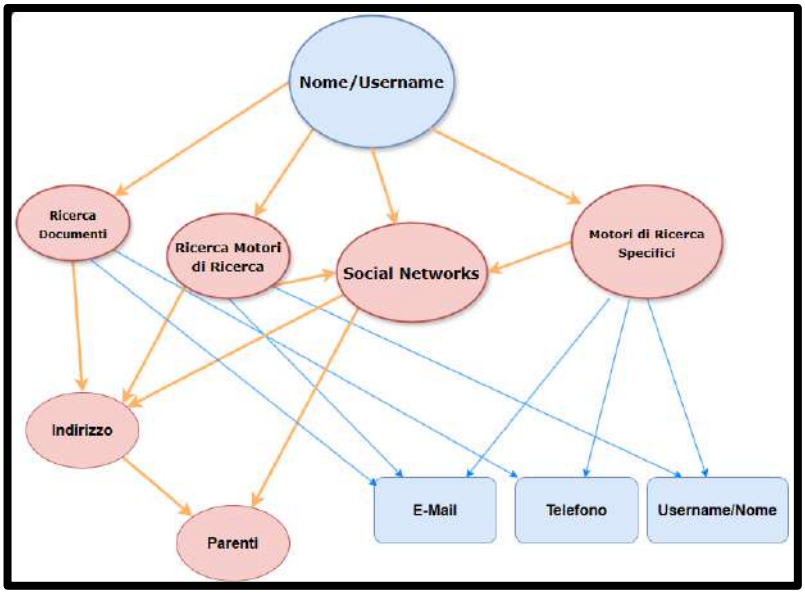


Figure 28:- Username Analysis Flowchart

Searching by a person's real name can be tiring and frustrating. If your goal has a common name, it's easy to get lost in the results. Even a fairly unique name yields nearly 20 people's addresses, profiles and phone numbers. If our goal is called *"Marco Rossi"* (a full common Italian name), we have a problem. This is why we should prefer searching by email address or phone number when available. This is among the first activities to carry out in order to search for the name and surname that interests us on the main search engines, such as Google, Yandex or Duckduckgo. But if we want to optimize the search and possibly identify specific documents such as public competitions or CVs, we can use Google Dorks or go to the main social networks we talked about in the previous chapters.

These are some tools that we can use to carry out searches knowing only the name, surname or 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. GoogleDork

Google Dorks are advanced search “queries” that can help you find specific or hidden data in the Google search engine. But they can also be used to recover sensitive data or identify vulnerabilities etc.

For example, you may be able to find a person's curriculum vitae or a company's tax return, expense reports from a municipal administration, documents relating to public competitions with the personal data of the participants. Details that may not appear on their websites or appear when you perform a routine web search.

Below is a list of some Google Dorks[3]which can be used to search for documents:

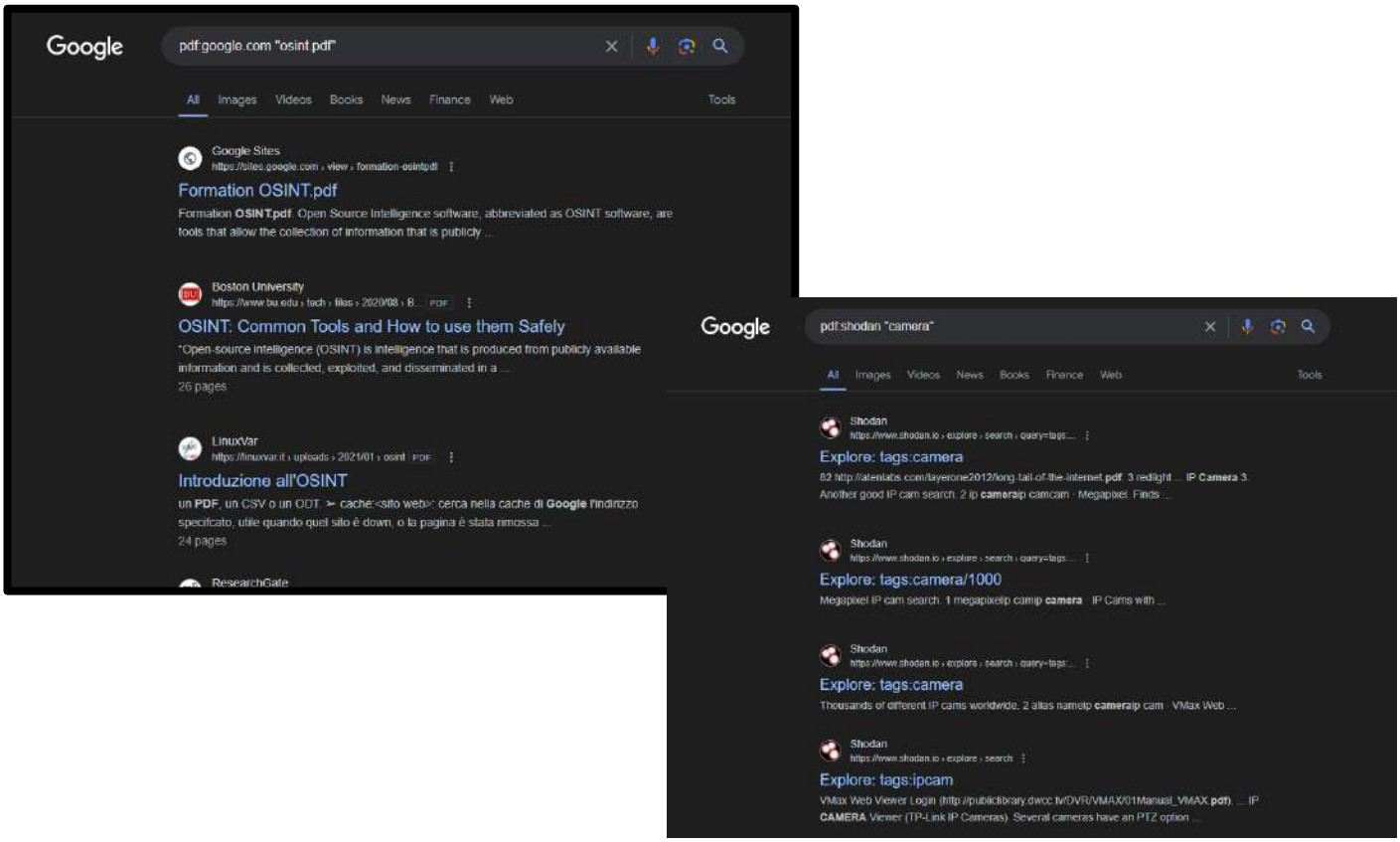


Figure 29:- Example of search using Google Dorks

[3]In addition to the tools listed above, below by following this linkhttps://github.com/CScorza/OSINTInvestigation/blob/main/-%207000%20-%20Google%20Dork.txt you can find more than 7000 google dorks that can be used for searching for different more specific purposes.

General PDF search	site:example.com filetype:pdf
Search for PDFs with specific titles:	intitle:"desired topic" filetype:pdf
CV search:	intitle:cv | "curriculum vitae" filetype:pdf | filetype:doc
Search for CVs by geographic area or skill:	intitle:cv "engineer" | "developer" | "designer" location:italy filetype:pdf | filetype:doc
Search for CVs on specific sites:	site:linkedin.com | site:indeed.com "curriculum vitae" | cv filetype:pdf | filetype:doc

If we want to use something that makes it easier for us to use *Google Dork*, we can use the following web pages, which allow us to carry out more precise searches:

- **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/

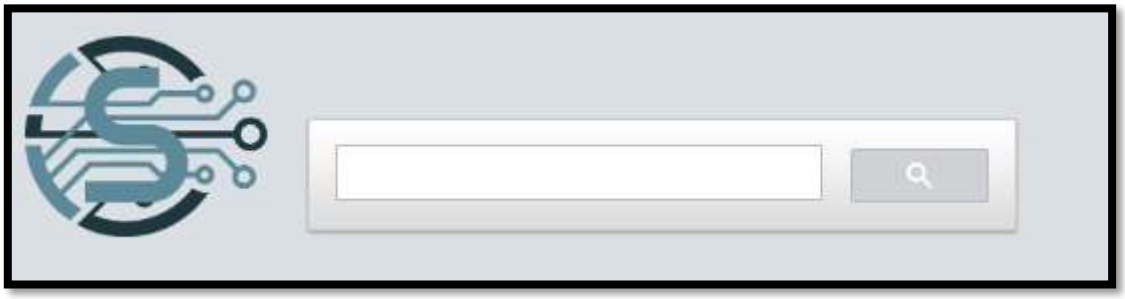


Figure 30:- CScorza Search

13. AANALYSIS OFAND-EMAIL

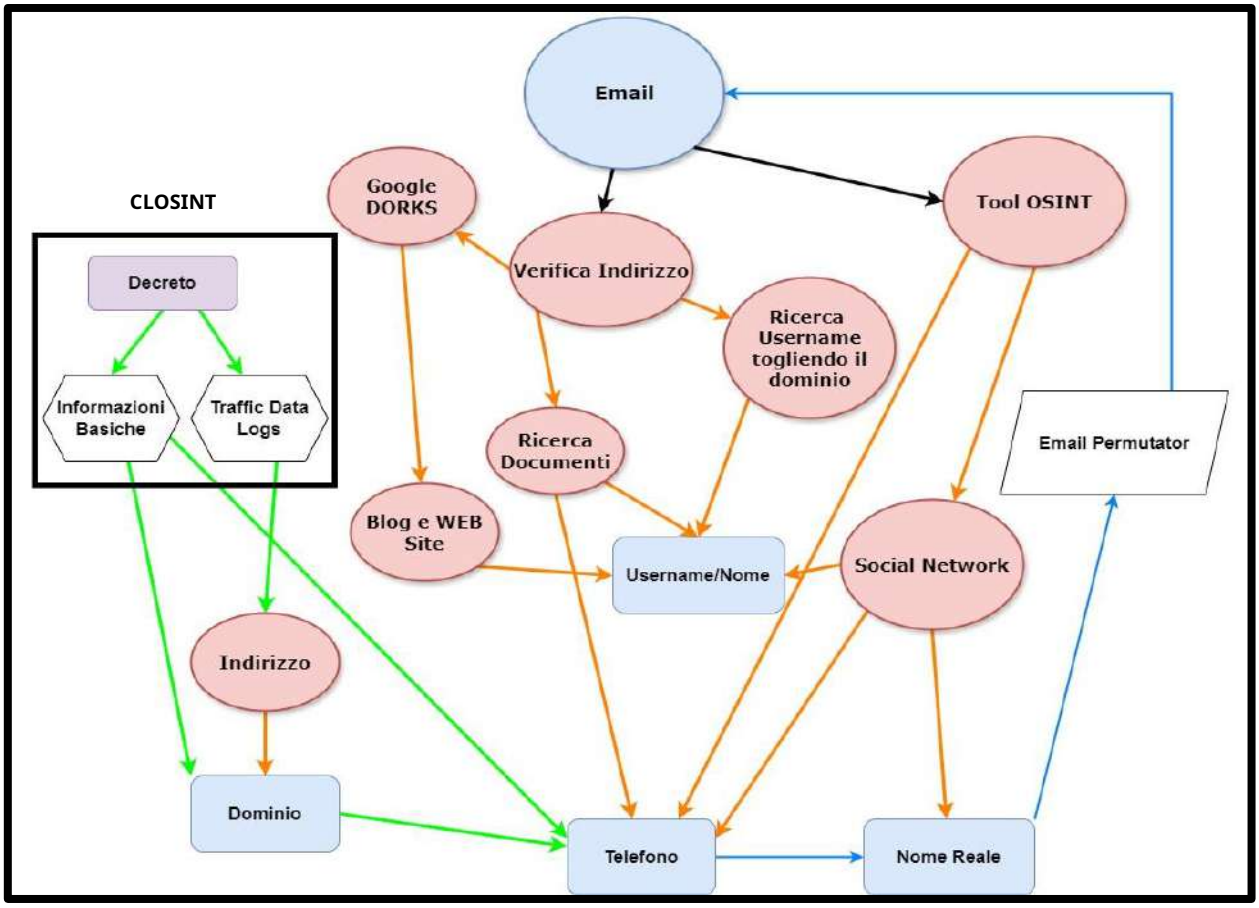


Figure 31:- Email Analysis Flowchart

It may happen that we know the email address of our target and we want to understand a which services is connected in order to obtain the real information of our target such as name and surname and telephone number, etc. As can be seen from the flow chart (Figure 21), we can carry out various steps to achieve our purpose, including including the "Google Dorks" as we have seen previously but also the use of free or paid OSINT tools that can provide us with a series of results that are useful to us. Among the various tools that we can use to carry out these types of checks we have:

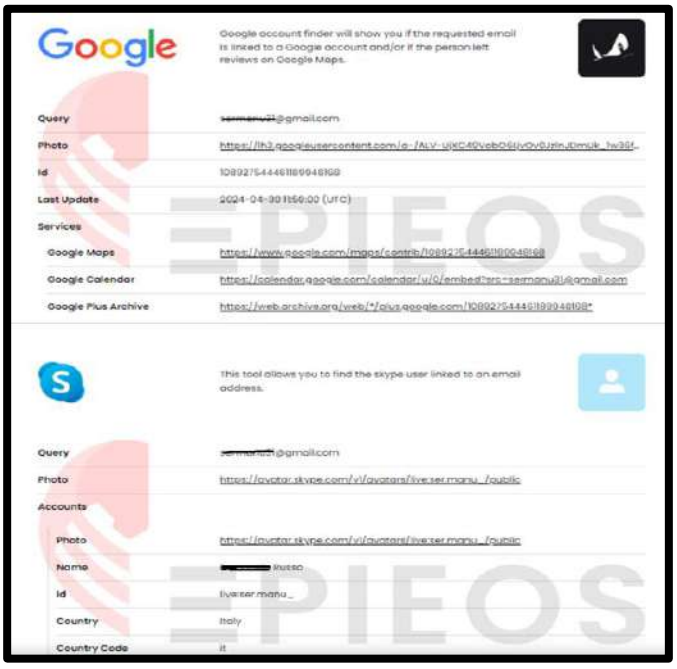


Figure 32:- Epieos

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

In fact, these tools offer the possibility of checking which social networks or web services the email is inserted into, managing to provide further data such as the name and surname and the profile image (see Figure 21).

14. AANALYSISNOUMER OFTELEPHONE

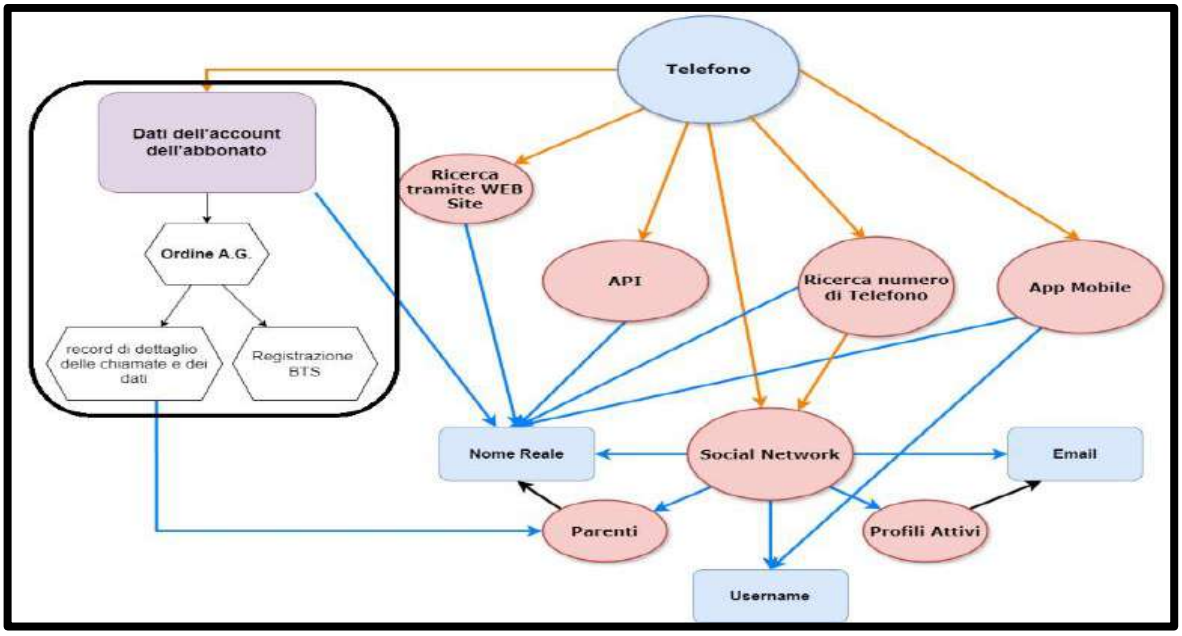


Figure 33:- Flowchart Telephone number analysis

If we have a telephone number, we can carry out three activities to find its user:

1. Identify what type of number it is and its provider; therefore, understand if we are dealing with a landline or mobile phone number or a "data" type number. Also, understand the supplier whether it is local or overseas.
2. Identify any user information such as first and last name and any associated residential address and email.
3. Finally, we can search for various services that are directly linked to the phone number, such as messaging apps (WhatsApp, Telegram), social networks etc. All

this will inevitably lead to further information that can help us to broaden our research.

There are various tools that can be used to analyze telephone numbers, some of which we have already encountered previously, such as**OSINT Industries, Epeios**And **Castrick**.

In addition to these, there are other tools that allow us to analyze a mobile number such as:

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

These applications[4]they allow you to carry out searches on any mobile telephone number, providing the name of its user as information. Furthermore, they also give the possibility to check if the phone number is registered in the most common messaging platforms such as WhatsApp.

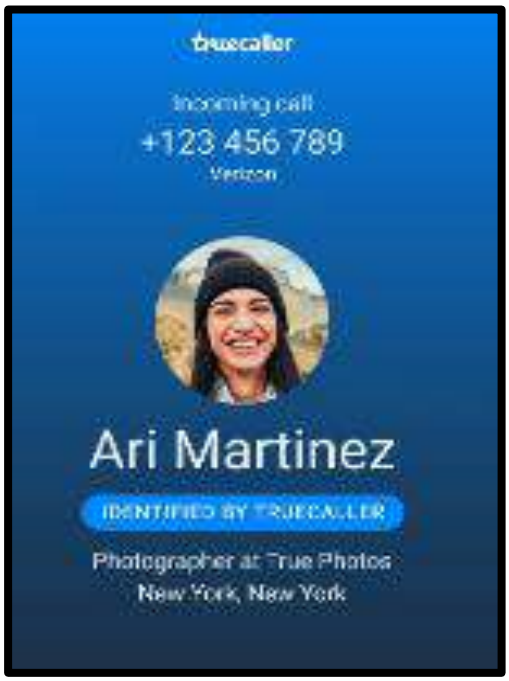


Figure 34:- Truecaller

[4]It is important to note that these applications require access to your phone's address book. Therefore it is advisable to use these applications with caution, for example using an Android VM, Android Studio, or an old phone without phone numbers saved in the address book.

CONCLUSIONS

Throughout this manual, we have explored in detail Open Source Intelligence (OSINT), a dynamic and ever-evolving field. We started with a historical overview, which made us understand how important it has always been to collect data and information for various nations over time. We have also outlined the various branches of OSINT and the importance in the modern context.

We have distinguished between Active and Passive OSINT, highlighting the monitoring techniques and tools useful for each modality. Next, we delved into the “Pivoting Method”, a fundamental process for the effective OSINT workflow, allowing you to easily move between different sources of information to build a complete and accurate picture and insert it into the final report.

The distinction between *Clearweb* And *Deepweb* it allowed us to better understand where to operate and how to access less visible but equally relevant and important information. We have examined the use and installation of a VPN to ensure not only the security and anonymity useful for protecting our data, but also improve the search for information.

The importance of password management, an indispensable tool for keeping access credentials safe.

The creation of a dedicated workstation, as well as the choice of suitable operating systems between Linux, Windows and Mac, are crucial steps to establish a safe and efficient working environment.

We then examined browsers and search engines, with a particular focus on Tor Browser, Mozilla Firefox and Brave, and the use of extensions to improve privacy and security while browsing, as well as to collect data during our browsing .

The section on Social Media Intelligence (SOCMINT) has provided a detailed guide on the creation of avatars (sockpuppets) for infiltrating and gathering information in social networks, covering various aspects such as biography, profile picture, e -email and telephone number.

Furthermore, we focused on exploring specific platforms such as Facebook, Instagram, X/ Twitter, LinkedIn and Telegram, highlighting techniques to make the most of them.

The analysis of usernames and real names, together with the use of Google Dorks, has shown how to extract valuable information through advanced searches.

The analysis of emails and telephone numbers completed the set of tools available for effective OSINT research.

In conclusion, this manual provides a comprehensive and practical guide for anyone wishing to enter the world of OSINT. Knowing and knowing how to use these techniques not only expands our information gathering capabilities, but also prepares us to navigate the complex digital landscape with greater confidence and awareness.

BIBLIOGRAPHY

- *"Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information" by Michael Bazzell*
- *“Deep Dive”: Exploring the Real-world Value of Open Source Intelligence 1st Edition*
- *Various courses taken online.*
- *Constant update*
- *Constant comparison with other OSINT and Intelligence analysts.*

All human beings have three lives: public, private and secret.

- **Gabriel García Márquez**

“CScorza”

Expert in Open Source Intelligence Techniques and Methods.
Through the GitHub profile and the Telegram Channel opened in 2022, it collects OSINT, Digital Forensics and Cyber Security software and tools. Within his Telegram channel “CScorza – Indagini Telematice”, he keeps his GitHub repositories updated with new techniques and tools for over 20 different topics.