Chapter

Private Investigation and Open Source INTelligence (OSINT)

Francisco José Cesteros García

Abstract

Social Networks has changed the way of developing an investigation as far as people use to explain, graph, show and give details about their life. It is so because people need to communicate and need to share feelings and passionate life. Based on these facts, private investigation uses the information in public databases to make an approach to people, their facts and their details that they publically expose to the rest of the world. So, this chapter explains how to use the OSINT (Open Source INTelligence) methodology for legally become part of the steps on a private investigation. The information is growing up and people expose their images, comment and reference to other ones so it facilities the investigation of getting results. Actually OSINT is the first step that private investigation must consider and this chapter covers and explains why and how to do this.

Keywords: OSINT, investigation, social networks, private investigation, private detective

1. Introduction

In the age of technology, obtaining information is basically a matter of managing search engines, having a working methodology, knowing how to correlate data and later, drawing conclusions [1].

It is obvious that the information circulates and is not always true, has biases and must be analyzed with prudence and know-how. Anyway, fake news is part of our life, up to day.

Therefore, in the discipline of intelligence analysis, there are multiple methodologies to generate information products with which to make decisions in personal and business life.

One of the mechanisms is what we call "the use of open sources", or in other words, using Open Source INTelligence (OSINT) [1], which becomes a basic part of the research, which must be carried out with care and methodology, avoiding biases and finally verify the information in the field.

Undoubtedly, OSINT is an essential element in the investigation, both previously, to be able to "get an idea", and to go deeper into fundamental aspects of the person or company investigated.

However, the belief that the information is free is not the case and the use of the following premises should be considered in an OSINT analysis [2]:

- Free information sources.
- Sources of payment information.

- Information sources with annual subscription.
- Time spent in the search, analysis and generation of the final product.
- Time spent verifying or biasing the information obtained.

Therefore, far from being a low-cost, low-profile intelligence product, OSINT research requires professionalization of the investigator and:

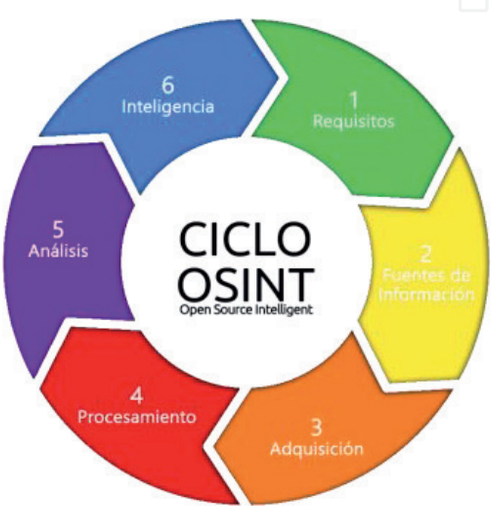
- Investigator's training.
- Identify sources of use and use credibility, bias and veracity of the information.
- Annual subscriptions with the implicit cost.
- Work methodology.
- Computer tools for the correct analysis, data correlation and generation of the final product [3].
- Research discipline.

Intelligence is the base of success in all fields. Intelligence is used for the military, political, business, and of course private level and investigation. Currently, all organizations and companies, of a certain level, use Intelligence to start, develop, and succeed [4].

If a supermarket wants to expand and locate in another country, it will first have to obtain all the legal, economic, structural, and competitive data, in order to make a decision. In this way it can decide the most suitable country for its investment. We can imagine any other type of business that wants to develop internationally, and it will have to follow the same steps.

Intelligence is used practically since human existence. But, obviously, the OSINT is much more current, since the new technologies have allowed this type of research in Open Sources [5]. And there are more and more research possibilities in this regard, because there is more and more public information available to everyone.

That is why it is essential in the process of obtaining information, to take the utmost care not to leave a trace, since if not, we will go from being analysts to being objects of investigation.



The basis of the Intelligence process is obtaining information. And the first step to obtain information is to search in Open Sources, known as OSINT.

The basis of the private investigation is getting the proof, based on experience, know-how, methodology, sources, man in the field and legal process [6]. So, we are moving on a briefly discovery of these elements and processes on this chapter.

2. Searching information in open sources

During the process of the investigation we will always find two different handicaps that should be taken in consideration:

- Amount of information: Need to be limited.
- Quality of information: Data that are not relevant and should be classified.

As in any research process, it is necessary to follow a methodology to obtain results. The OSINT intelligence cycle follows the same methodology as the intelligence cycle, but using Open Source Research tools.

This is the OSINT process [5] we follow in a private investigation:

1. Requirements: Determine which ones are the objectives to investigate. What information is needed to obtain.
2. Information Sources: Establish the information sources that will be needed to obtain the information and, if payment information is required, take into account the cost involved.
3. Acquisition of Information: Search for information in established sources.
4. Processing: With the information obtained, the necessary reports will be made, extracting the useful data for the pursued objectives, and with the same rule of the 3 "C's" that is used for Press News:

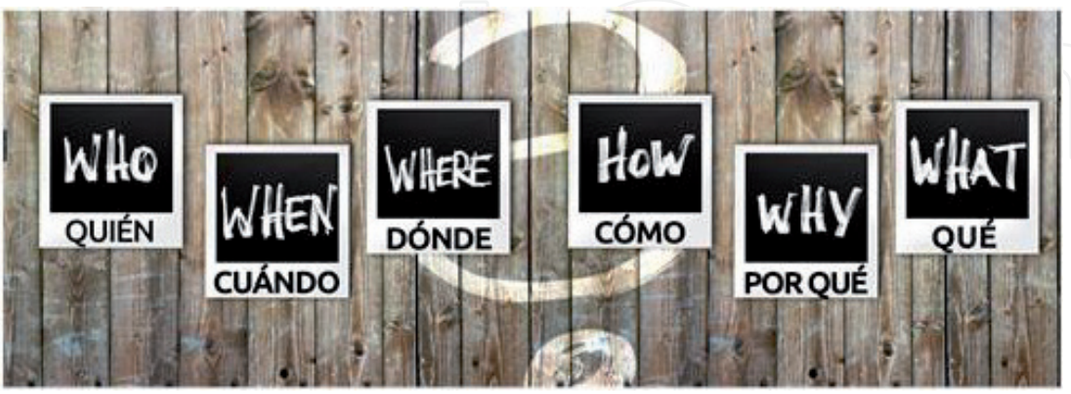
   Information needs to be:

   - Clear
   - Concise, and
   - Concrete
5. Analysis: Once the reports are completed, the information obtained will be analyzed, giving meaning to the data found. What they mean for our interests.
6. Intelligence: The analysis will determine the actions that we must carry out based on the information obtained.

We have to give answers to the following questions:

- Who?
- When?

- Where?
- How?
- Why?
- What?



Some of the answers are gotten from the OSINT investigation [5] and traces the way for the field investigation, but, we have always to consider the credibility of the source and the reliability of it.

The information is coming from different sources (with its own reliability and credibility) and should be checked and not taken as valid information [7]. Disinformation is part of what people and companies usually do.

Because of it, the OSINT process has to consider this classification methodology (see **Table 1** below).

As a result, each piece of information is classified and evaluate, answering the big "W's" as follow:

Example: Evaluation of the source: B/2, A/1, C/3… [8].

2.1 Type of open sources (for OSINT)

Once we have written about open sources, let us explain the reader where we can search and make the investigation, as an example, but it is not limited to these sources [9]:

- Internet search engines [10] (most used search engines: Google, Bing, Yahoo, DuckDuckGo, Ecosia, IxQuick, Ask, Lycos, Yandex, Dogpile, Startpage, Peekier, Webcrawler, Yippy, Exalead, Factibites, Wayback Machine, Gibiru, Siri, Alexa, etc.) and using the logical operators they have.
    - Google Dorks and its Boolean operators, symbols and commands can be used for explicit and specific search.
        1. AND, OR, NOT, XOR: (example: thread AND jihadism)
        2. (): (example: (thread OR terrorism) AND (islamism OR jihadism)
        3. Operators: *, #, ¿, $, €, "", for example
        4. Symbols: <, >, =, <>, <=, >=

Reliability	Credibility
A – Completely reliable	1 – Confirmed by other sources
B – Generally reliable	2 – Probably
C – Reliable enough	3 – Possibly true
D – Generally unreliable	4 – Doubtful
E – Unreliable	5 – Unlikely
F – Cannot appreciate reliability	6 – Credibility cannot be appreciated

Table 1.
Reliability and Credibility of information sources.

5. Commands: define: term; filetype: term; site: site/domain; link: url, etc.

6. And many others operators of each engine.

- Websites, Forums and Blogs from different countries and languages based on the information we are looking for, the people, the specific information and themes.

- IP [11] and Device locators (networks, open ports, webcams, printer and many other IP devices): Shodan.io, Myip.es, Ip-address.com, Iplocation,net, Httrack.com, Pastebin.com, Whois.com, Robtex.com, IANA, RIPE, etc.).

- Social Networks [12] (Youtube, Vimeo, Instagram, Twitter, Facebook, Pinterest, Reddit, Vkontakte, Tumblr, Linkedin, Infojobs, Snapchat, and so many others including those for Contacts and Couples like Meetic, eDarling, Badoo, etc.).

- Maps (internet) and Geolocation of data (Iplocation.net, Coordenadas-gps.com, Mapsdirections.info, Mapscoordinates.net, etc.).

- Magazines (different languages, countries and specific search engines based on the information and goals we are following).

- Newspapers (exactly the same as before).

- Conferences where people could participate, even in academic, public or private that are published in corporate webs.

- Radio and Television broadcasts

- Official Gazettes and Registration: Civil Registration, Penalties Fee Registration, Property Registration, Commercial Registration, etc.

- Organizations: Professional Associations, Professional Colleges, NGOs, etc.

- Mobile applications: WhasApp, Skype, Telegram, Signal, etc.

- Emails pages that we can use them for generating a temporal email [13] or for looking in case the accounts could be hacked (Pastebin.com, Haveibeenpwned.com, Shodan.io, Verifyemailaddress.org, Mxtoolbox.com, Toolbox.googleapps.com, Mailnator.com, Guerrillamail.com, Temp-mail.org, Correotemporal.org, Throwawaymail.com, Maildrop.cc, Mailnator.com, etc.).

- Images scanning: By looking for images in internet and checking the metadata and location or even a possible fake image of a profile (Google Images, Bing, Tineye, Yandex, Revimage.com, Pictriev.com, Exiftool, Fotoforensics.com, Photo-forensics, etc.).

These sources of information can be classified into:

- Free databases and registers
- Free databases but profile requirement
- Free databases but real profile and request (for example a death certificate)
- Payment sources

And many others tools that frequently appears and disappears in the internet world [14]. Basically talking, we are opening a tremendous world of investigation where, as talked before, know-how, experience, technical knowledge and legal procedures must be under consideration.

As the reader can image, the gather of information is a tough procedure that requires different use of tools, technical background and methodology for the identification, analysis and classification of the information.

And this is part of the education and training that private detective should get as part of the evolution, the state of the art and the success of the private investigation agency (so, the business itself).

But, who can we work for getting the information without been discovered? This is part of the next point.

3. Secure investigation using legal tools

Social Networks (SN) are an unimaginable source of information [15] and that makes them an ideal place to locate relevant information on the topics to be investigated.

However, not everything that is on social networks, not even what each company or each person puts is real. Various considerations:

- Each one says what he wants for personal interests.
- Not everything that is said is true and must be checked.
- They have a bias based on who the information is directed to.
- They can also be forwarded fake news.

Therefore, as a premise, and highlighting what we have already been exposing to the reader throughout the chapter, the sources, in this case, social networks (SN), must be:

- Evaluated
- Classified
- Collated

And this is the relevance of having a research, evaluation, classification and methodology for investigating inside the sources.

Many photos, videos and texts are posted that, at first glance, seem real and interesting, but when it is necessary to analyze to make a report, it is convenient to check because if not the credibility of the analyst, remains low if the information has not been verified, and may have financial and legal consequences within an investigation.

Once we have put these premises ahead, we must also remember a legal aspect [16] that is more than important, the usurpation of identity.

> *"Identity theft, also called the crime of usurpation of marital status or identity, consists of the action of appropriating a person of the identity of another, posing as her to access resources and benefits, acting in legal traffic pretending to be the person impersonated. The action described in the criminal type is to usurp the civil status of another".*

Because of this penal action [17], the way remains to build ad-hoc profiles for research. And this is part of the investigation process, methodology, time and technical resources.

On the other hand, the creation of profiles must meet clear objectives:

- Be according to the goal to be investigated.
- Do not use copyrighted or other people's photos.
- Take specific photos and edit them so that they are consistent with the case and can reflect interest for the person or company to investigate.
- Profiles are created, fed and populated and when done they are simply dropped.
- Research profiles are not recyclable. They should not be used in other investigations.
- They must be created in safe places or with non-traceable media.
- They have to show relevant information for the investigation and reliable content for the investigation.
- When you do not reach people directly, you have to look for an alternative route through friends or interests, you have to build the necessary coverage.
- The coverage, direct or indirect, must also be attractive to the goal of the investigation.
- The profiles to be created and the names to be used must be in the language, culture and form of expression of the group, person or sector of the company. You have to take care of the contents and make them credible, including other languages.
- And assign specific cellular phones to the investigation and contact.

Once you decide to undertake an investigation obtaining information from social networks, you must consider:

- What SNs are the appropriate ones for this type of investigation, since Facebook is not the same as LinkedIn, Twitter or Instagram, but there are many as we have introduced early before.

- Consider the ages of the people to be investigated and their origins, since ages mark one or another SN and cultural origins as well.

- The profiles can use the same name in all of them, but perhaps it is worth reflecting on whether for a specific investigation, it is better to use different names in different SNs in order to complement information or avoid blocking.

So with these working premises, and knowing that creating the profiles, feeding them and having them ready to work takes a long time, it is good to consider and keep in mind that:

- Investigations into SN sources take a long time.

- They require prepared profiles, which take time to create and provide adequate content.

- They are not fast.

Some recommendations to be considered:

- It is used to create emails and profiles on social networks when you are traveling, because with them created and saved, they are from different cities or non-native countries and are very useful for investigations and traces of them.

- Provide the profiles that you create with certain information of interest so when the operation of investigation is launched, takes less time and reflects more seniority in the profile.

- Manage information in the profile according to the name, interest and content with which we want to use it later.

The usual formulas to obtain information in SN are:

- Use previously created profiles that have content according to the topic to be investigated.

- Contact the people or companies to investigate using these profiles created ad-hoc.

- Use safe navigation and if possible outside the home.

- If necessary, purchase operator cards and use your mobile for internet connection instead of ADSL at home/office.

- Extreme security measures in communications and traces, firewall, incognito and secure browsing, do not leave traces in search engines or even use a cyber coffee or telephone booth.

- Make friends with the person or company and also seek common interests, common friends and provide credibility and a high number of friends and common acquaintances.

- If possible, illustrate with edited photos the contents of the profile to give it greater credibility and seriousness.

- If it is not possible to get a friendship directly, you have to think about:

  - Go through other friends, family, etc.

  - Have topics of interest to this person and express it so that they accept.

  - Refine the profile created with aspects of interest to your contacts in such a way that they are the ones who introduce us.

So with these recommendations and advises, let us talk something about three other secure things to consider:

- Internet Address (IP) and Virtual Private Networks (VPNs)

- Secure browsing

- Email creation

3.1 Internet address and virtual private networks (VPNs)

Another aspect that should be exposed and that says a lot in the investigation of open sources and the obtaining of information, is to obtain the IP [18], or at least, to know from where the entries can be produced, not always easy, and much less when try to follow criminals.

Although obtaining the IP of the people to investigate is difficult, our IP could be also traced and the relevance of the investigation is the security of the agent.

For that reason, we must protect our IP address using different methods:

- Using SIM cards and mobiles that we can throw (at least the SIM card) when we have finished the investigation. This SIM card must be "not traceable" or at least not our name or agency registered.

- Using Virtual Private Networks (VPNs) [19], technology that (free or payable) allows us to connect to internet using a tunnel where our IP original is converted to another, protecting in this way, our location and identity.

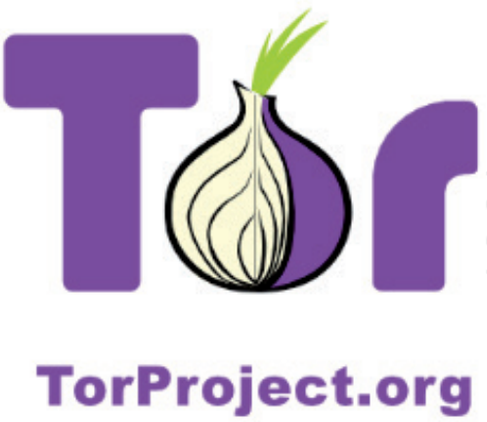
- Using TOR (dark web browser), which uses a VPN and relays to jump between one to another node in the internet world.

As per using one or several of these mechanisms we can make the investigation by securing our access and blocking our connection, direction, and location to others. This is the first step, to protect our location and work on locate the investigated people.

As we have briefly explained in point 2.1. of this chapter there are different tools for executing the IP investigation and there are different tools of VPN software for laptop and mobile to protect ours.

3.2 Secure browsing

The software mostly used for this kind of investigation is TOR browser, which refers to The Onion Router (TOR) Project [20].



This navigation is what we call, *The Dark Web [21]*.

A part of the deep web consists of internal networks of scientific and academic institutions that form the *Academic Invisible Web*, which refers to databases that contain technological advances, scientific publications, and academic material.

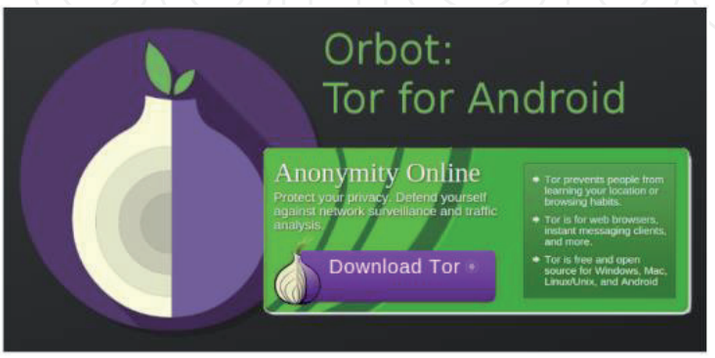
But there are more services published in this dark web:

- Financial services: bitcoin laundering, stolen PayPal accounts, cloned credit cards, banknote counterfeiting, anonymous money wallets, etc.
- Commercial services: sexual exploitation and black market, stolen gadgets, weapons and ammunition, false documentation and drugs.
- Anonymity and security: instructions to enforce privacy in TOR, especially for a sale or in bitcoin transactions.
- Hosting services: web hosting and image storage where privacy comes first. Some prohibit uploading illegal files and others have no restrictions.
- Blogs, forums and image boards: apart from those related to buying and selling services, two frequent categories of this type of community are hacking and the exchange of images of all kinds.
- Mail and messaging services: some email addresses are free (generally they only offer webmail) and others are paid, with SSL and IMAP support.
- Hacking services: of websites, emails and paid.
- Political activism: censored file sharing, hacktivism, and even a page to organize "mass-funded assassinations." Anarchy is the predominant ideology on the deep web.
- State Secrets: There is a copy of WikiLeaks on the deep web, and several pages where to publish secrets with little activity.

- Books: virtual libraries that measure several gigabytes and contain thousands of ebooks in different formats. Many of them are free of copyright and others are illegally distributed in direct download.

- Erotic pages: paid and free access. The subcategories are diverse and without any moral limit.

Investigations not always require getting into the deep web to look for information, but at least require protecting ourselves from being located. Using the protection of the IP and using an incognito browsing and VPN (TOR for example) we use a double layer of protection who isolate us from being detected and pursue.



In this moment of the lecture, we have enough information to understand risks of the investigation, technical knowledge we require and evaluate the investigation as a professional way of working, not for amateurs and with time to be paid for.

3.3 Email creation

Adding to the previous point, not enough as many webs and search process require an email address; we have to mention something like the creation of emails accordingly, again, with the goal of the investigation.

The registration to create a social network profile requires an email address, and perhaps, depends on the SN, a mobile number.

¡Never use your personal profile or cellular number!

The creation of an email, some years ago, was tremendously easy and limited, not today that we have a lot of services for creating temporal emails or real email for working alone.

But, again, to create an email account, we need an internet connection, so please, remember the previous recommendation, ¡protect your IP! by using the recommendations.

You cannot create a profile in social network using TOR, you cannot create an email account using TOR, but you can protect your IP address by using any other technologies (VPN for example), or using a cyber coffee or when traveling, creating the email account from the hotel. In this way you preserve your home/office IP address.

Once you are sure that your IP address is not conducting to your real IP, then you can use the temporal email accounts creation we have exposure in the point 2.1 of this chapter or you can use the Google, Hotmail, Yahoo, etc. services for it.

The goal is to create a secure email for using temporally to create the SN profile, or not so temporal, to be used contacting with the investigate people or company so it can be left when finished.

However the creation of an email account is very simple, keep in mind what you need for your investigation:

- Email account to be used only for SN profile creation.
- Email account to contact with the investigated.
- Email temporally account.
- Email of a known service provider to give some more credibility.
- Email with a specific goal in mind.

4. 360° surveillance

It is very clear, in this page of the chapter, that we are generating digital tracks continuously and because of that, we are creating a digital footprint [22].

Once again, to follow up the footprint of a person requires methodology, knowledge and technical resources for the investigator.

360° surveillance consists in monitoring the footprint that a person, profile, email, etc. (all of them resources of the internet world) are leaving while writing, browsing, using internet from any device.

People use mobile phones, tablets and laptops for accessing resources, services and use the internet applications so the device is another footprint.

It means that the device has an operating system, a geolocation, a camera, a timetable of use and so many characteristics.

Monitoring with methodology we can use the information of the footprint to determine, for example, but not only:

- Where the investigated people are.
- How is using the SN profiles.
- When they are mostly connected.
- Which device is mostly used.
- Some characteristics and operating system of the device.
- Sometime way tracking to office.
- Habits and mostly frequently zones or restaurants.
- Comments they write in Blogs and shopping references.
- Determine the style of life.
- Determine if they are always in the same location or move during the weekend and where.
- When they write, where are they writing.
- Etc.

A lot of information is part of this footprint that can be follow up with specific tools and because of the device connection to internet.

360° surveillance is not only monitoring the people investigated and can be done for monitoring family members also, so it creates a big hole for VIP people.

If someone wants to track and monitor the life style or life of an executive, for example, can be done by contacting directly with them or through different profiles, including their children or friends.

Because of public profiles of executives and VIP people in SN, they are exposed to be monitor by any people, with or without a real profile. Part of the investigation that private detective can do is the counter surveillance.

Counter surveillance looks for monitor who is accessing specific profiles, claim for friendship and contact with their victims.

The 360° surveillance can be executed by any person, with good or bad intentions, for example to discover habits, where the person is, life style, if they are at home or vacation, or used for making some scratches, strikes, disturbances, etc. against the company, the executive or to follow up a singer, a football player or disturb them at a disco.

These are some examples, but we leave the reader imagine what can a person do with information of other, for good or bad things.

Based on the reality of the digital footprint, the counter surveillance looks for a protection of the person and their family in order to continuously monitor their network activity, search for any news and alerts, and protect the digital image, the physical person and guarantee the integrity of the information, the person, the family and the corporate image.

360° surveillance and counter surveillance is intended to protect people and companies from scams, scratches, damage to the image reputation, and of course to protect their exposure perimeter.

Open sources, company's news, blogs, social networks, emails, etc. are part of the sources that give a lot of information to others, including criminals, and private detective try to protect their clients of all these risks, not only on the field, either in the digital field.

We are always leaving digital tracks to other by:

- Using different communication channels through internet services.
- Actors that interact with our profiles.
- Activity we realize on internet by purchasing, navigation, cookies, profiles, alerts, etc.
- Blogs, Chats, Recommendations we leave.
- Contents we visit.
- And do not forget that you mobile continuously interact with Google (Android account, Samsung Account) or Apple (iCloud).
- Using cloud storage (Google Drive, iCloud, Dropbox, etc.)
- Sharing images of vacation, for example.
- Sharing the training routes and records.

- Using Youtube.
- Using Google account by default without blocking some services.
- Etc.

Hopefully for the reader, the private investigator has the knowledge to protect companies and private persons, family and friends also and to train, investigate and offer security once analyzed the exposure perimeter, the risk and the goals of the people/family or company.

Private investigation agencies are focused on exactly that, protect and investigate their customer, and in this technological times, digital tracks are part of the protection and investigation that is mostly required.

5. Conclusions

After reading this chapter we expect that the reader has a very clear knowledge of what a private investigation agency can do for their security and what is the way of working for getting the information through the internet services and methodology for searching, before going to the field and certify the information gotten.

It is obvious, after reading the chapter, that everyone is having a digital track at least for having a mobile phone connected to internet and this digital connection generates a risk.

The risk is part of the evolution and it is part of the technology. Nothing is 100% secured but we can and we must put the resources to protect ourselves and our family.

WiFi (Wireless Fidelity) at home is another hole of security, especially as most of the routers installed have not changed the password and default passwords are on public technical webs.

By accessing the WiFi at home, every single device connected to it can be hacked and of course information of the devices, stolen.

Profiles, passwords, emails, and devices are objects of desire for criminals and private investigation agencies should improve their investments and knowledge to adapt their detectives to new technologies and methods.

Private Detectives are used to work on the field but in this times, the first thing should be look for information by using OSINT techniques, analyze the information and then verify this on the field. It gives the detective a better understanding of the information and investigation and allow them to be cheaper and more professional.

Of course, OSINT is not the only way of working as many people do not have profiles or share information or do not like to navigate, but OSINT should be the first step in any investigation to have any more information, even the lack of information is, of course, information.

Detectives need to recycle and clients need to understand that OSINT investigation takes a lot of time and should pay for it. It is a mix between working in an office and working on the field. The time required for each kind of investigation need to be considered, evaluated and put in place while preparing the offering to the client.

Open Source INTelligence and Private Investigation have a lot of things in common and both are part of the world of getting information, complementing each other.

It requires methodology, technical resources, education, time and experience to move on private investigation without trespassing laws and be able to add value to a field investigation and success of the customer on a trail.

Acknowledgements

The author declares no conflict of interest.

Special thanks to my family, colleagues and company that give me some time to write and develop the chapter.

It took some personal time for structuring, develop and write it and this time has been stolen to all of them.

Thanks to the editor for allowing me to write an specific chapter of private investigation and how it can help people and companies to success and follow up situation of conflicts and negotiations.

From the private investigation sight, I wanted to explain the methodology, steps and legal process in order to let readers know that the investigation is something serious, professional and it is far from movies and amateurs who makes things happen for entertainment or for getting some illegal money with criminal offenses.

Author details

Francisco José Cesteros García
Cuzco Detectives, Madrid, Spain

*Address all correspondence to: fjcesteros@cuzcodetectives.com

References

[1] INTelligence. Open Source Intelligence. 2010. Available from: https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/open-source-intelligence.html [2020-11-28]

[2] OSINT, the power of the information. 2014. Available from: https://www.incibe-cert.es/blog/osint-la-informacion-es-poder [2020-11-28]

[3] Practical Open Source Intelligence methodology. 2012. Available from: https://medium.com/seconset/practical-open-source-intelligence-methodology-4ddc57eac917 [2020-11-28]

[4] Ciclo de Inteligencia. CNI. Available from: https://www.cni.es/es/queescni/ciclo/#:~:text=Se%20entiende%20por%20Ciclo%20de,%2C%20Obtenci%C3%B3n%2C%20Elaboraci%C3%B3n%20y%20Difusi%C3%B3n. [2020-12-30]

[5] Defining second generation Open Source Intelligence. 2018. Available from: https://www.rand.org/content/dam/rand/pubs/research_reports/RR1900/RR1964/RAND_RR1964.pdf. [2020-12-30]

[6] Servicios de Investigación privada. Derechos y obligaciones. 2020. Available from: https://cuzcodetectives.com/servicios-de-investigacion-privada-derechos-y-obligaciones/ [2020-12-30]

[7] ¿Qué son y para qué sirven las fuentes de información OSINT? 2020. Available from: https://papelesdeinteligencia.com/que-son-fuentes-de-informacion-osint/ [2020-12-28]

[8] Source evaluation and information reliability. 2015. Available from: https://www.first.org/global/sigs/cti/curriculum/source-evaluation [2020-11-28]

[9] "Must have" Free resources for Open-Source Intel (OSINT). 2020. Available from: https://www.sans.org/blog/-must-have-free-resources-for-open-source-intelligence-osint-/ [2020-11-28]

[10] Top 12 best search engines in the world. 2016. Available from: https://www.inspire.scot/blog/2016/11/11/top-12-best-search-engines-in-the-world238 [2020-11-28]

[11] IP Location. 2020. Available from: https://iplocation.com/ [2020-11-28]

[12] 95+ Social networking sites you need to know. 2021. [2021-01-05]

[13] 7 servicios de email temporalis. 2016. Available from: https://www.genbeta.com/correo/7-servicios-de-email-temporales-para-evitar-spam-y-otros-problemas [2020-11-28]

[14] OSINT Framework. 2020. Available from: https://osintframework.com/ [2020-11-28]

[15] Las redes sociales como Fuente de información. 2012. Available from: http://portal.uned.es/pls/portal/docs/PAGE/UNED_MAIN/LAUNIVERSIDAD/VICERRECTORADOS/GERENCIA/IUISI/COLABORACIONES/076%20DOC_ISE_08_2012.PDF [2020-11-28]

[16] La usurpación de identidad. 2015. Available from: https://www.legalitas.com/pymes-autonomos/actualidad/articulos-juridicos/contenidos/La-usurpacion-de-identidad [2020-11-28]

[17] Suplantación de identidad, tipos y causas. 2019. Available from: https://protecciondatos-lopd.com/empresas/suplantacion-de-identidad/ [2020-11-28]

[18] IP Address. WhatIsMyIP. 2020. Available from: https://www.

whatismyip.com/ip-address-lookup/ [2020-11-28]

[19] ¿Qué es una VPN? 2020. Available from: https://www.xataka.com/basics/que-es-una-conexion-vpn-para-que-sirve-y-que-ventajas-tiene [2020-12-30]

[20] TOR Project. 2020. Available from: https://www.torproject.org/ [2020-11-28]

[21] Qué es la Dark Web, en qué se diferencia de la Deep Web y como puedes navegar por ella 2020. Available from: https://www.xataka.com/basics/que-dark-web-que-se-diferencia-deep-web-como-puedes-navegar-ella [2020-12-30]

[22] Your digital footprint: What is it and how can you manage it?. 2018. Available from: https://www.rasmussen.edu/student-experience/college-life/what-is-digital-footprint/ [2020-11-28]