OFFENSIVE INTELLIGENCE

Philippe Dylewski

This book is a compendium of tips, tools and techniques for finding out everything about everyone, in the corporate world and beyond. This practical manual will teach you how to conduct a professional investigation, both in the field and on your computer. You will learn the secrets of Google Hacking and the dark web, and also how to locate a person with a simple photo, an e-mail address or a telephone number. You will know everything about the real-time situation of your competitors and partners.

Philippe Dylewski is a trained psychologist. He ran a recruitment agency before becoming a private detective, then a business intelligence specialist. He now lives in Thailand and coordinates the activities of a group specializing in the search for missing persons throughout the world. He has published several manuals and novels in France and Belgium.

ISBN: 979-10-96819-29-4
EAN: 9791096819294

AGAKURE

OFFENSIVE INTELLIGENCE

Philippe Dylewski

Philippe Dylewski

OFFENSIVE INTELLIGENCE

300 techniques, tools and tips to know everything about everyone, in companies and elsewhere

Second edition

AGAKURE

Philippe Dylewski

OFFENSIVE INTELLIGENCE

300 techniques, tools and tips to know everything about everyone within companies, and elsewhere

Second edition

TABLE OF CONTENTS

Translated from French by Evelyn Balikanda

I. Introduction

The first edition of this book dates back to the year 2010. At the beginning, it wasn't meant to be a book but a manual that I was creating little by little, to help me in my job as a private investigator. The lovely lady I lived with at the time pointed out to me that while spy novels were in plenty, spy manuals were not.

I did a rough layout, and I had 100 copies printed at the copy service, down the street. All of the copies were sold out within a week. A few months later, tired of stamping and enveloping, I wanted to try my luck with publishers. Since I didn't know any, I used an address collector robot that I launched on Google. At the end of the day , I had more than 5,000 email addresses of French publishers . The accuracy of the addresses was not great, for I had addresses of manga publishers, that did children's' books or books about land. I used an emailing platform and in one hour, everything was sent with a nice letter and the book's summary.

Within a few weeks, I had received six contract proposals and I eventually signed with "L'Express", a famous French publisher. Needless to say, they did a good job. They produced a wonderful book, promoted it and I had the narcissistic pleasure of going around to bookstores to see if they had my book in stock. The only drawback was that the book dealt with a sensitive subject and for legal reasons had to be edited. At the time, it seemed normal to me, that a publisher would want to protect himself from possible prosecution. I haven't changed my mind, however, if I wanted to write a truly offensive book, I had to feel free to be able to write whatever I wanted, including the worst. That's what you're starting to read.

This book is for professionals such as:

- Private investigators, intelligence and strategic intelligence specialists.
- Journalists.
- Marketing managers.
- SME managers.
- Recruiters.
- Law firms.

It is not intended for IT security managers or digital marketing gurus. On the one hand, they won't learn much in their sector, and on the other, this book deliberately places itself in the shoes of the attacker. It is not intended to protect your computer network or to help you sell on Amazon nor any other online store.

The goal is simple: to provide tools, techniques and methods that give you access to information about your competitors, suppliers, customers, employees and business partners. From what I see on a daily basis, my clients often make important decisions based on very little information. A good balance sheet, a nice resume, a little sympathy, and instincts do the rest. A good balance sheet does not mean much, a great resume can be bogus, and your instincts could be fooled.

I've often heard executives say things like "I don't care what my competitor does; I don't look at what my neighbor does". That's a noble attitude, but it doesn't seem to me to be any different from the officer who sends his men into battle without knowing anything about the enemy.

In no way do I advise spying on competitors in order to copy them, only to do better and to avoid being left behind. Monitoring your competitors is about learning from their strengths and weaknesses, what works and what doesn't. It's about learning and growing.

This manual that you are holding in your hands is intended to be easy to use. You will be offered hundreds of tips, methods, tools and links. Excluded from this book are anything related to programming and anything that requires a high level of technical knowledge. Expensive tools are also excluded. This his is a manual and therefore mere reading will not be enough; you will have to work and practice. Without that, it will be useless.

II. In-depth research on Google and Google hacking

1. The search engines

The basis of remote intelligence is **Google** . It's a must that you use it. Google is currently the number one search engine in the world, though it has one major drawback: it tracks your activities on its own behalf, or on behalf of third parties. Of course, you have nothing to hide, which means that you're not likely to be walking around naked outside your window! Simply because we have nothing to hide, does not mean that we agree to bare all.

Remember that you are using this manual for spying purposes, and that you may have to make requests that could one day have unfortunate consequences. Fortunately, you will be told later how to anonymize your searches.

Google is not uniformly present all over the world. China and Russia have their own alternative search engines and if you have investigations to do in these areas, it will be essential to use those. We will soon see how to overcome the language barrier.

Baidu is the leading search engine in China, with a share of over 70% of the Chinese Internet market.

The statistics diverge on this subject - It has more or less the same design as Google. If your investigation is within China, you may have no choice. Beware that Chinese search engines are heavily censored and if your search has political connotations, there is a big chance that you will not find what you are looking for. This engine is only of interest if you can make queries in Chinese. https://www.baidu.com

I can't resist showing you that I have a book translated into Chinese. If I do the same search on Google, I can't find this link. In the figure above, the search is conducted using our alphabet while I simply wrote that a query on Baidu must be written in Chinese. This is a special case, where the book translated into Chinese has a cover in Chinese, but the author's name is written in both alphabets.

Yandex is a search engine widely used in Russia, and is the market leader. https://yandex.ru/ is in Russian only but allows searches in English or French. This will not help you much; but if you are looking for specific Russian information, you will get it only by asking in Russian. We will see later that there is an intelligent translator that will solve your ignorance of Chinese and Russian for good.

There are many other search engines. The best known are; **Bing, Yahoo** or **Ask** . Others are less well known but offer a guarantee of discretion. Some are even environmentally friendly, at least according to their managers.

Bing really has a strong point compared to Google: its cartography is of a better level and its video search is more user-friendly. Apart from that, Google is still the master of the world.

2. The basic search

Google has access to less than 10% of the total web, 90% of the rest belongs to the invisible web, and it’s known. The same has been said about the human brain, that we only use a small part of its potential. What is certain is that there is so much information out there, that if you don't have sorting tools or do a thorough search, you won't find exactly what you are looking for. Google uses a ranking system called **PageRank** to rank search results from most relevant to least relevant. In fact, the more a site's address is listed

by other sites, the more relevant that site is. Each link pointing to a page is considered a vote for that page. This means that when you conduct classic queries, you will find that the most popular results are not necessarily the most relevant.

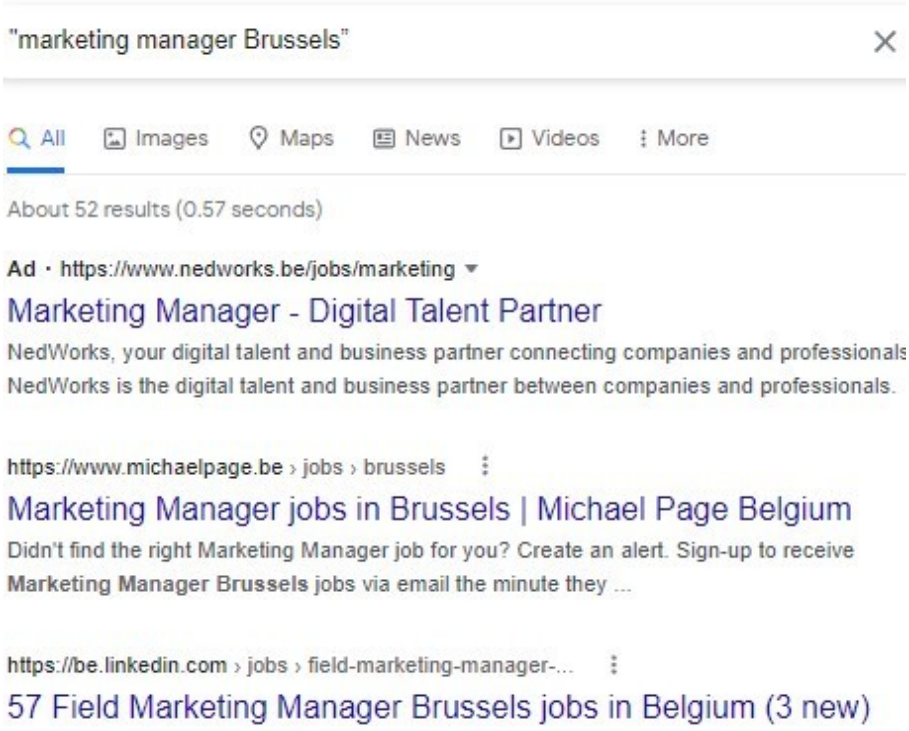
That's why you're going to become **Boolean search** pros. Boolean search is a query method that allows you to broaden, narrow or refine your search results. In the recruitment field, Boolean search allows you to quickly and efficiently locate ideal candidates for job openings. Similar to an "advanced search" function, Boolean search operators allow you to include, exclude and tag specific keywords to carefully refine your search results. Ultimately, the purpose of using Boolean search in recruiting is to refine broad topics such as job titles or requirements to identify a pool of candidates.

All the following will be especially helpful when you're looking for something specific that needs to be sorted. If you're looking for an old girlfriend whose first and last names are quite original, don't bother with the following., but if you're looking for Tom Cruise, an electrician in the south of Alabama, or your target's probable ties to a company, read on.

The quotation marks (“”)

This is the very first thing you need to know when searching on Google. A basic rule that you should repeat every time you search for a specific expression. Quotation marks allow you to search for a series of words or names in a very specific order. For example, if you type "marketing manager Brussels”, you will only find links to these 3 words. The same query without quotation marks can lead you to very different pages where marketing will be mentioned but where the terms "manager" or "Brussels" can appear for any reason.

Quotation marks are obviously used to search for information about a person or an address: "first name last name", "address postal code, city". This was especially true a few years ago. Today, if you type "Philippe Dylewski" as opposed to, Philippe Dylewski, the first results will be the same, but when a query becomes complex, the quotation marks " " becomes indispensable.



When I make the same request without quotation marks, (" "), the first results are almost identical. The difference is that instead of receiving 28 results, I receive more than 7,000,000. This is because very quickly, I receive links to pages including the word "marketing", "manager" or "Brussels".

Cached pages

When Google scrawls the web, it creates a copy of each page it examines and stores it in a **cache** , allowing you to view this copy at any time, especially if the original page is not accessible. When you click on the "cached" link on a web page, Google displays the page as it was when it was most recently indexed. In addition, cached content is what Google uses to determine if a page is relevant to your queries.

When a hidden page is displayed, it is preceded by a boxed header that reminds you that this is the hidden copy of the page, not the original page,

and cites the terms of the query that led to its inclusion in the search results. To make it easier to use this page, the different occurrences of the search terms are also highlighted in different colors.

The "cached" link does not appear if the site has not yet been indexed nor if the site owner has requested that the cached content be excluded from Google indexing.

All this is really only of interest if the page has disappeared from the web which happens very often or if you want to get email addresses from a PDF document.

Indeed, most of the address bots are not able to extract data from a PDF file, yet if you manage to open the document with the "cached" mode, you can achieve your goal, ergo, it is a very useful feature.

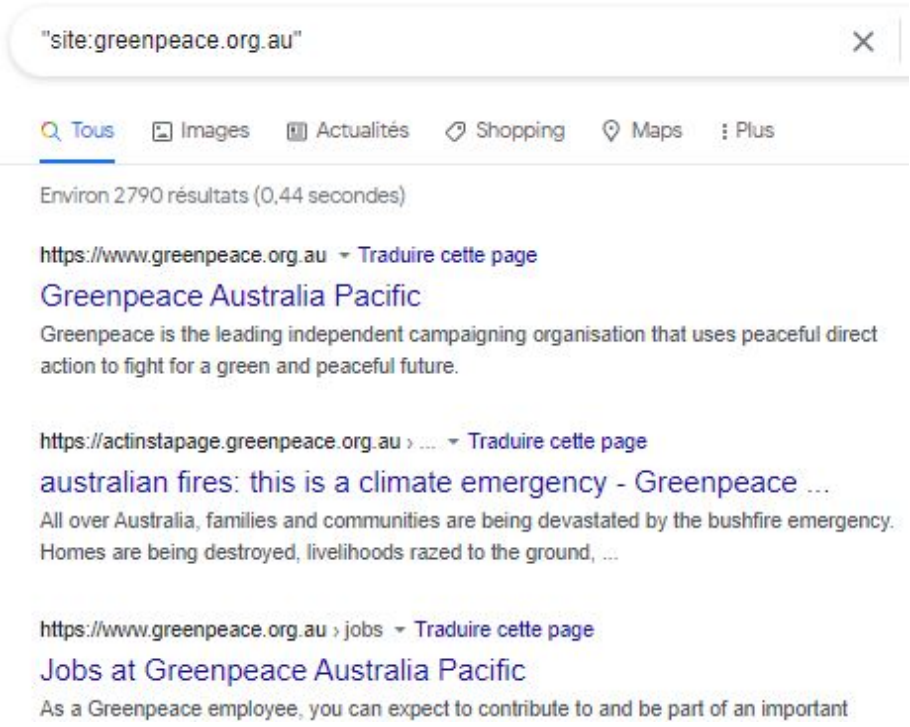
Punctuation and capitalization

For Google, writing in upper or lower case makes no difference. There is no need to crack your head. The same goes for punctuation, hyphens and other cedillas. Google does not recognize them. Even the (@) sign is not recognized, which is a bit annoying when I search for an email address. Note that this is not necessarily true for other search engines. For example, Duckduckgo recognizes the (@) sign, which can be useful for some searches.

Restricting a search to a particular site

The information you are looking for is on a particular site. If you type in the URL address of the site (e.g. www.greenpeace.fr), you will of course be taken to the site. You will be taken to the site's home page and can begin your search in a sea of information.

If you Google "greenpeace.co.uk", you will get lots of links to Greenpeace. But if you use the term "site:greenpeace.org.au", you will only get links that lead to the Greenpeace Australia. Do not forget to type "site:greenpeace.org.au" without a space. If you leave a space, the formula does not work.



So far, the only advantage is to get a general view of the site to be studied. It's not bad, but not enough to start dancing the polka.

But if I want to do a precise search in a site, on a given theme or name, it is possible. In the following example, I search for references to Nicolas Sarkozy (former French president) on the Greenpeace.fr site and only that. With 431 results, I think we can say that at Greenpeace, they like, or they liked, to talk about Nicolas Sarkozy.

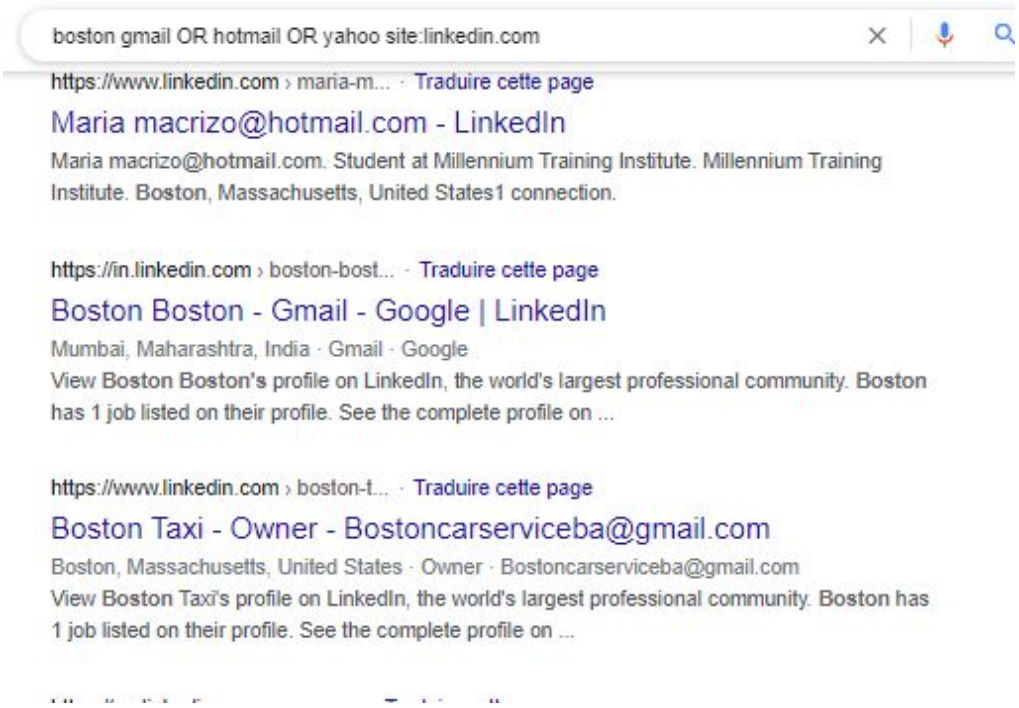
This tip is useful when you are conducting a search on a large site like when the information is on a newspaper or magazine site, even if you can get the same result from their archives.

You can use the **site** : function to do specific searches on your competitor's site. Be careful, nothing that you would not find by quietly scanning it. You save time. For example, if you want to know your competitor's rates, you type site: mycompetitor.com rates. If the rate is not on the site, no magic formula will find it.

One or the other

The "OR" used between two words or expressions will bring back all the links containing one or the other of these words or expressions. This saves you time because you don't need to conduct multiple queries.

In the following example, I'm trying to get the email addresses of people or companies in the Boston area with a LinkedIn profile.



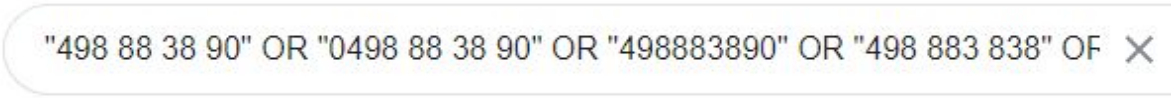
Don't think that I have discovered the secret formula to get the emails on Linkedin. I only find the ones that are on people's public profiles. This operator is also useful when you are not sure of your target's spelling. For

example dylewski OR dilewski OR dylevsky will return all results based on the different spellings.

Also in people search, this operator allows you to test different search variables in a single query.

"philippe dylewski" OR "dylewski philippe" OR philippedylewski OR pdylewski OR phdylewski

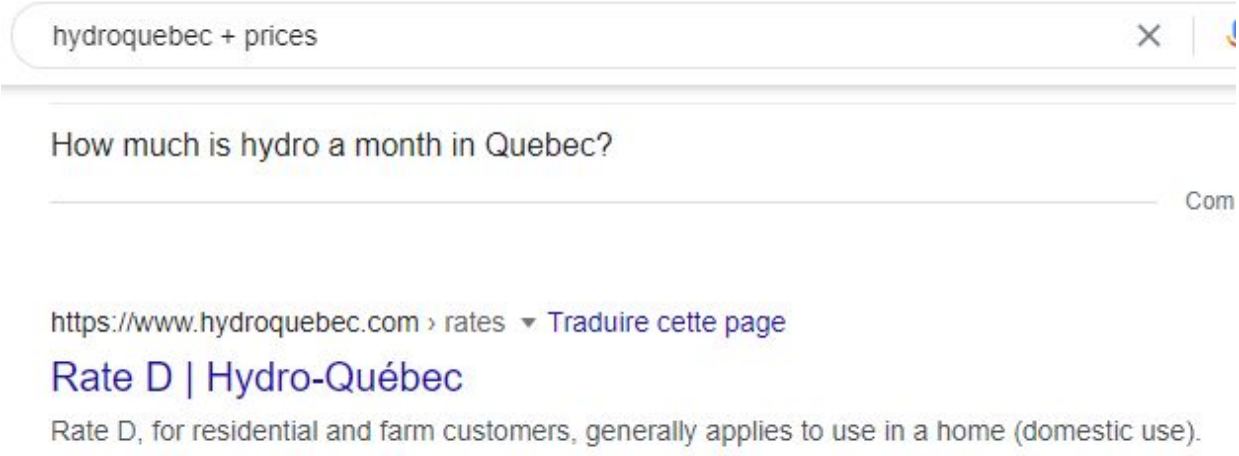
Finally, when you only have a phone number to find information about a person, the OR function is very useful since there are different ways to write this number.



This is the cell phone number I used until recently (Belgian number) and in two minutes, you can find my address and a link to different sites as well as a Facebook profile that can be traced back to me very quickly.

The one AND the other

The "AND" operator is no longer useful today because when your query is more than one word, the "AND" is applied by default, which was not the case in the past. There are still some small differences, but they are minor. What is interesting in the example below is the power of association of two words. I want to know the Hydro Quebec rates.



Searching for a keyword in the url

This Boolean criterion allows you to search for a specific keyword in the URL of a web page.

Example: in url:CV allows you to search for web pages with the word CV in the URL.

Another example, to find cameras without security code.

"Camera Live Image" in url: "guestimage.html"

Find a map

Maps: following a location allows you to immediately find maps for that location.

Tilde ~ The TILDE symbol (~) can be used to either expand or collapse your search results. The TILDE operator includes synonyms of the keyword you mark with this symbol in the results.

To find a salesperson's resume, you might use the following search string: ~CV "salesperson"

The search results will include all resume-like documents from the vendor profiles. If you run your query as is, you'll get a lot of garbage. You'll mostly come across job postings, or resume templates, or resume writing methods that guarantee you the job of your dreams. To avoid this, you can combine TILDE with the NOT operator:

~CV "seller" -template -example -job -method

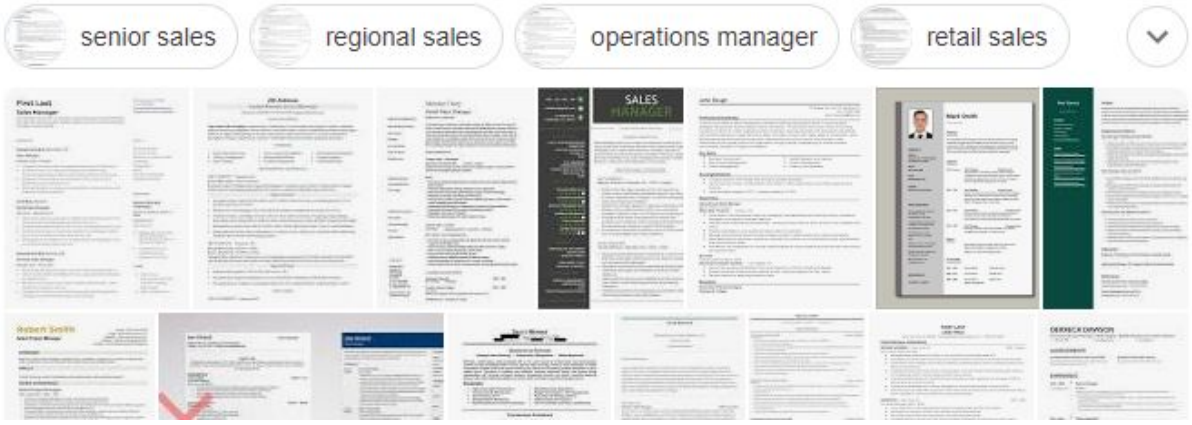
On Google, this search string will allow you to generate results containing mostly real salesmen resumes. You can also keep adding NOT operators to further reduce unwanted results.

NEAR

NEAR allows you to search for words (or phrases) that appear close together in a document or web page. It is a proximity search operator that will search for and automatically returns results containing key phrases separated by 1 to 10 words in the text.

For example, if you are looking for the resumes of sales managers who have sales experience, your search string might look like the following:

~CV "manager" AND (sales OR "sales representative")



A little oversight?

Feature: search for variations of a root word. Use the asterisk (*) operator to broaden your search results when you know there are multiple variations of a root word.

Example: To greatly expand your search results for a manager, searching for manag* will return results such as: manager, managing, management, manager etc.

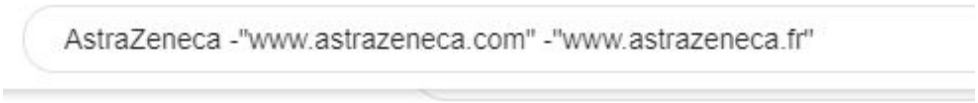
Be careful where you cut the root word, because adding an extra letter will change your results.

For example, searching for manage* will eliminate "managing" from the original list.

Exclude from your search

The "-" sign is used when you want to exclude specific terms or requirements. In the example below, I am looking for a sales manager or marketing manager living in Belgium but not in Brussels. Since I want to find potential candidates, I exclude job offers. Here, my search is on the LinkedIn website.

The exclusion is especially interesting when you are searching for a company but want to avoid all the pages that lead to the site of this company.



Here, I want to search on AstraZeneca, avoiding the different sites belonging to AstraZeneca.

32 words limit

Google only takes into account the first 32 words of your searches. I say this because it is rare to do a search with more than 32 words. If you still think it is necessary, develop your synthesis skills before coming back to this book.

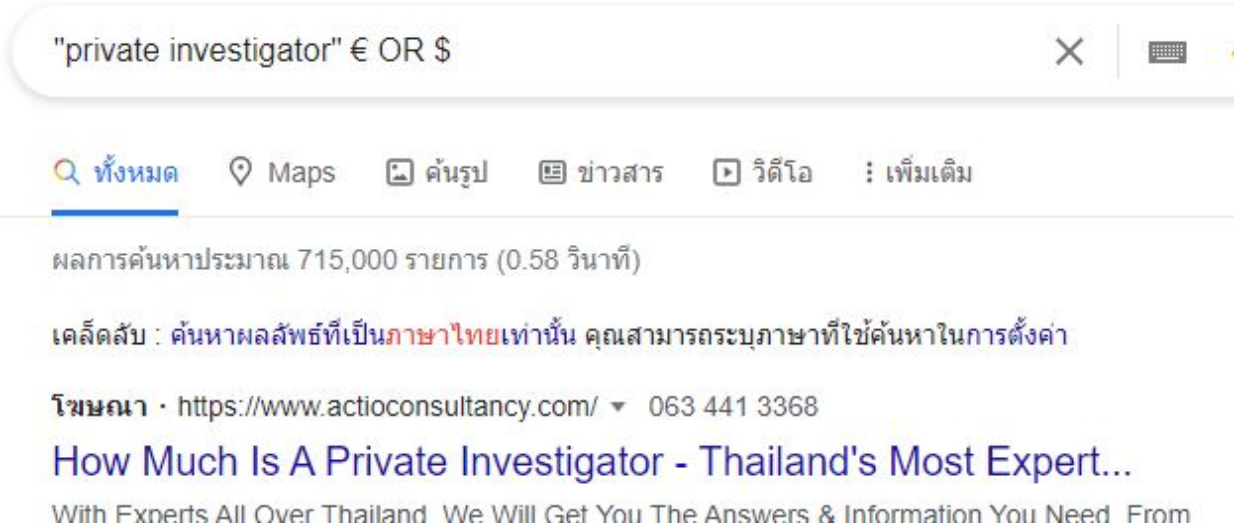
Conducting multiple searches of equivalent level

Parentheses ( ) group search terms or operators to help structure an advanced search

Google, not surprisingly, offers me specific links in all three countries. This operator saves a lot of time because when you have to conduct various queries of equivalent level, you do it in one go.

Search for a price

$ / €, this operator allows you to search for the price of a product or service.



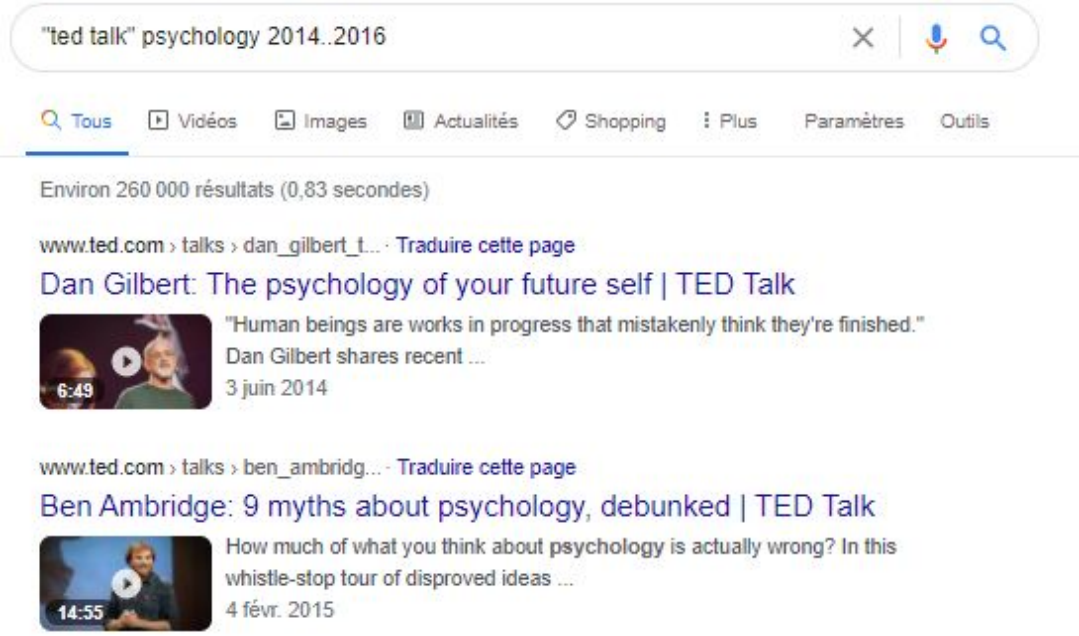
Here I get rates from neutral sources or private detective agencies.

Search from.... to....

PS4 € 10..80 Here I ask for the prices of the Play station 4, knowing that I am willing to pay between 10 and 80 euros. I receive a series of links to

second hand consoles. For this, I place .. between two figures.

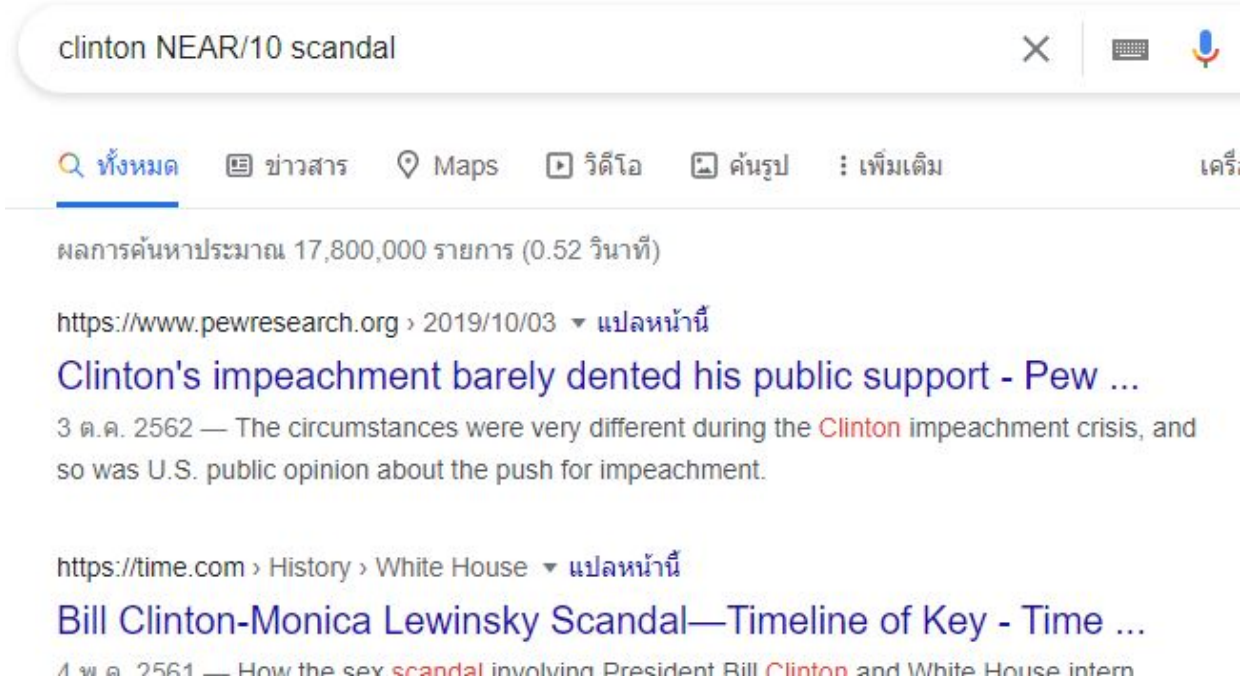
I could do the same thing if I search for Ted Talk lectures on a topic like psychology from 2014 to 2016. I get what I asked for first (2014). When I scroll down the list, I start to get Ted talks from other time periods.



The same technique can be used to search for credit card numbers or the inhabitants of a given street.

Common Context Search

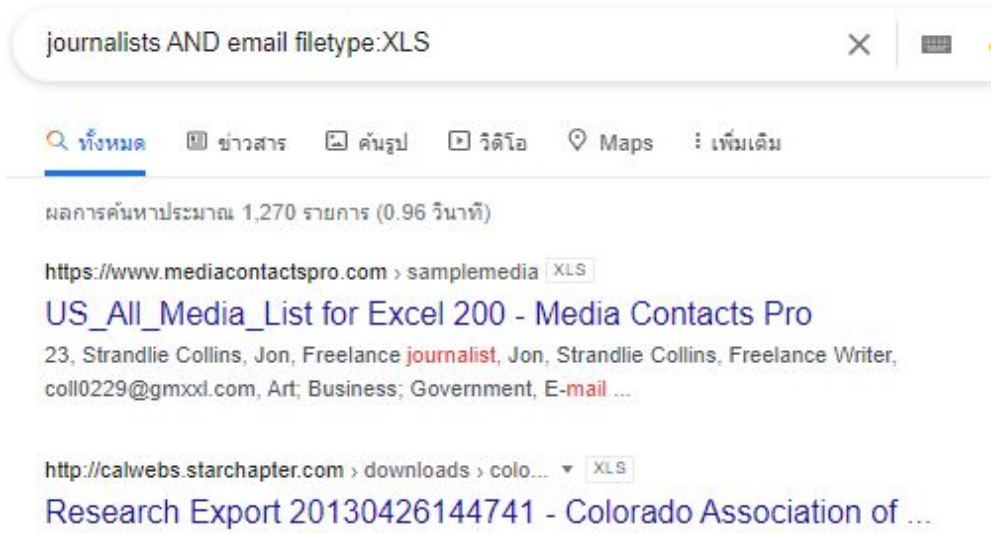
When you want two keywords to appear near each other in a set of results, you use the expression NEAR/12, which allows me to get all the links where these words are present, and at most, separated by 12 words. Of course, you can use any number.



Here, I am looking for information about scandals related to Bill Clinton. This option is very interesting when you are investigating links between two entities (people, subjects, companies...). If only to know if these links exist.

Searching for specific files

If your search is limited to a specific type of file, the "filetype" operator is for you. By adding this operator to your search, you can ask Google to return only one type of file in the results. For example, if you want email addresses of journalists, but only on Excel spreadsheets, this operator will do for you: journalist AND mail filetype:xls



This operator does not work with all file extensions but the most commonly used ones are compatible: i.e

Adobe Portable Document Format (.pdf) either filetype:pdf

- GPS eXchange Format (.gpx) either filetype:gpx
- HTML (.htm, .html, and other extensions) either filetype:htm
- Microsoft Excel (.xls, .xlsx) either filetype:xls
- Microsoft PowerPoint (.ppt, .pptx) either filetype:ppt
- Microsoft Word (.doc, .docx) either filetype:doc
- OpenOffice presentation (.odp) either filetype:odp
- OpenOffice spreadsheet (.ods) either filetype:ods
- OpenOffice text (.odt) either filetype:odt
- Rich Text Format (.rtf) either filetype:rtf
- Text (.txt, .text, and other extensions) either filetype:txt
- XML (.xml) either filetype:xml

Search in the title

The operator **intitle** : allows you to group all the results mentioning the keyword specified in the title of the page

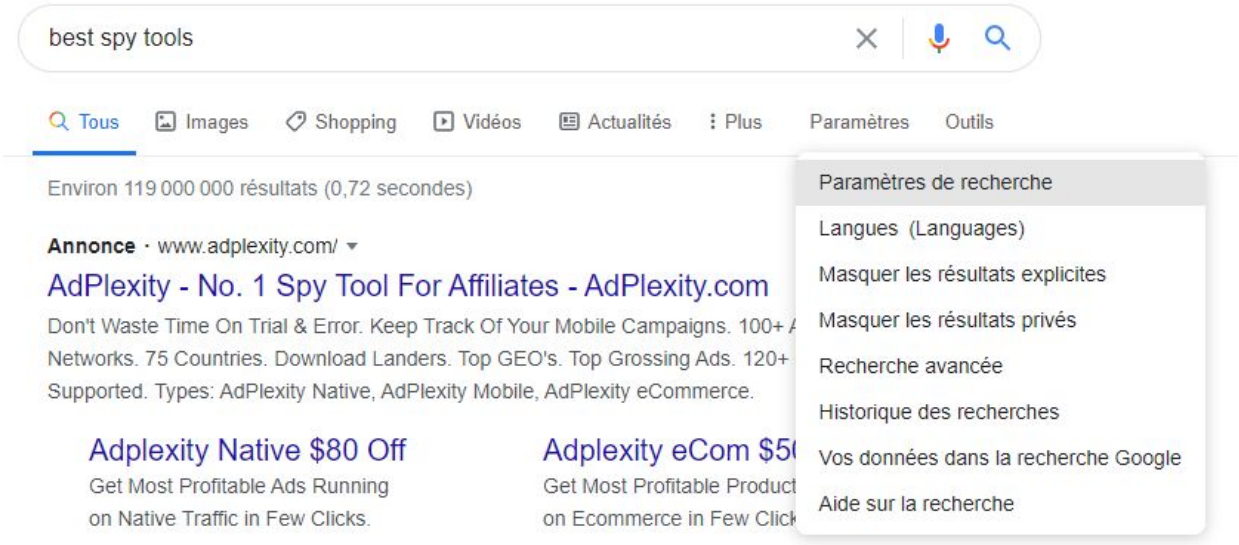
Example: intitle:(spying OR intelligence) will give me all the links to pages whose title contains the word "spying" or "intelligence".

If you are too specific in your search, the risk is that you will get nothing. That's okay, there's always time to broaden the criteria. If you search for documents about Volkswagen in German on the territory of the Congo, it might not yield much (I tried, and there is one anyway).

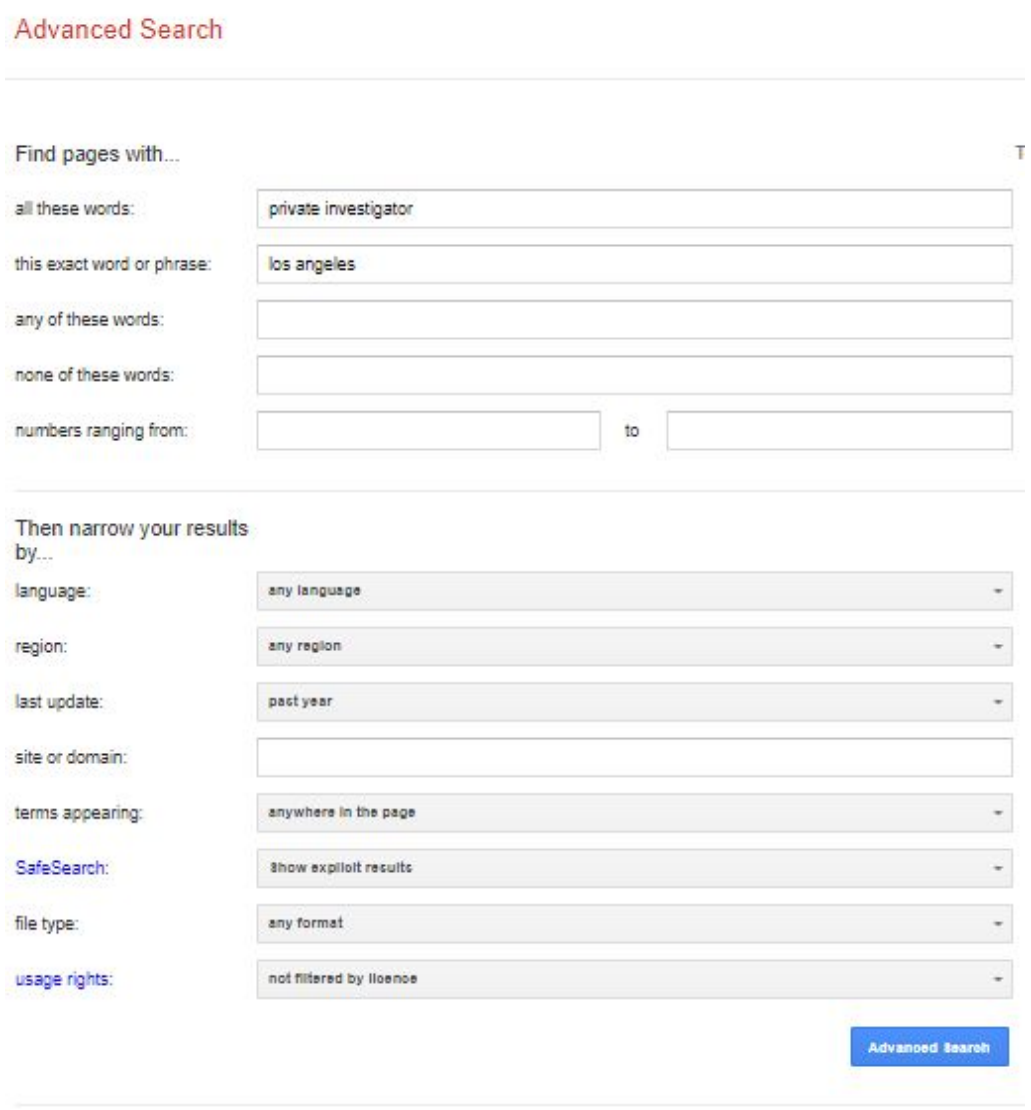
When you want to search in a given country, I suggest you use the national Google (google.fr for France, google.it for Italy...). The results will be both more numerous and better structured. In short, not all the Googles in the world are alike.

3. Advanced search

Advanced search is the automated version of Boolean search. It does almost everything but not everything. I invite you to click on the "advanced search" button. You can find it by clicking on the "settings" button, then "advanced search".



Its main advantage is that you don't have to learn the cabbalistic rules of traditional Boolean search. But if you want to become a real champion of information tracking, the advanced search does not exempt you from learning.



In this search, I need to find a private investigator in the Los Angeles, California area. It's a very simple search, and the results Google offers are exactly what I need. The advanced search gives me all the combinations of "AND" "OR" () - that I might need. Very handy. I might as well have asked to find a private investigator in California, but not in Los Angeles or San Francisco.

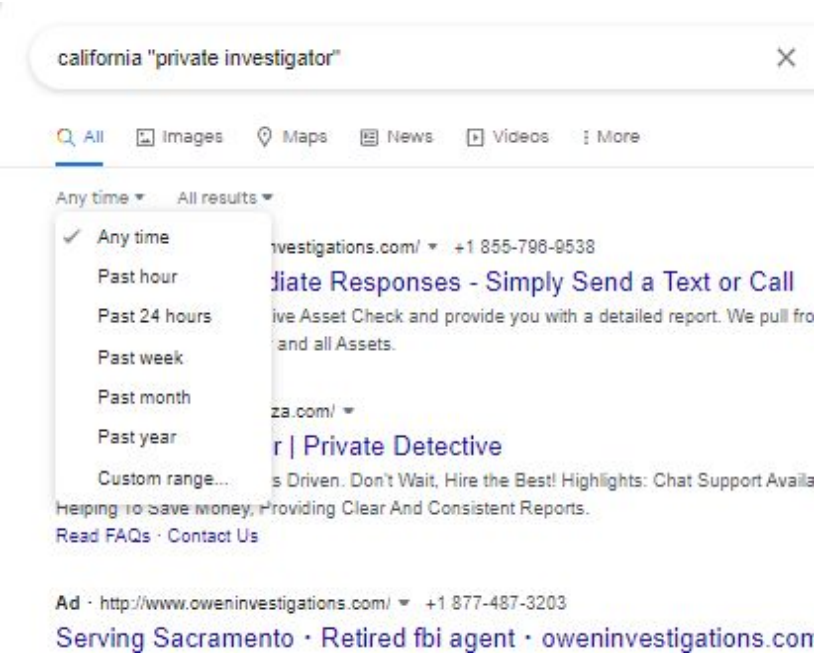
The engine allows me to search by language. This means that if you only speak French, nothing prevents you from requesting results only in French.

Obviously, with a search for California detectives, this is not likely to yield much. In fact, nothing at all. I can also search by region, which I advise you

not to do because a site can be hosted in any country. Nothing prevents me from having a French-speaking site in Thailand (which is precisely the case).

I can do a search based on the last update of the links. This option is a bit weak because you can either ask for the results of the last year, the last month, the last week, the last 24 hours or you accept that the date is indifferent to you. This means that if you want to get the results of the last two years, once your results appear, you will have to click on the "tool" button of Google and ask for the results according to the dates that suit you.

If you don't specify anything, "any date" will be the default choice and you'll get just about everything from the ancient days of Google.



You can also request that the search terms appear anywhere on the page, in the title, in the text or in the URL of the page. And finally, you can ask to receive only the existing links in a specific format (Word, Excel, PDF...), which is useful if you are looking for reports or databases for example.

4. Some offensive applications with Google Hacking

Google hacking, also called Google Dork or Google dorking is a valuable resource for investigators. For the average person, Google is just a search engine used to find text, images, videos and information. However, in the InfoSec world, Google is a powerful investigative tool.

You can't hack sites directly using Google, but since it has enormous web search capabilities, it can index almost everything on your site, sensitive information inclusive. This means you could be exposing too much information about your web technologies, usernames, passwords and general vulnerabilities without even knowing it.

In other words, Google Dorking is the practice of using Google to find vulnerable applications and web servers. I'm not kicking down a door, I'm letting myself in because it's open.

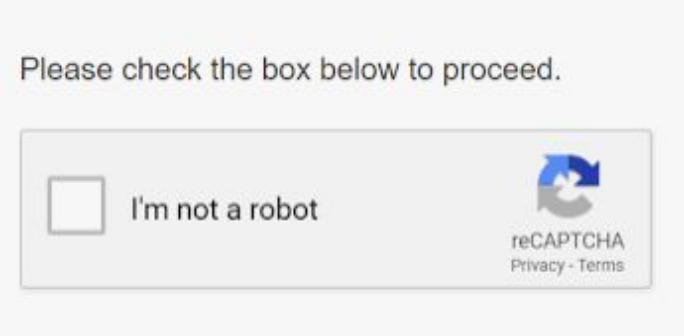
Unless you block specific resources on your website with a robots.txt file, Google indexes all information on any website. Logically, after a certain amount of time, anyone in the world can access this information if they know what they are looking for. You should know that Google also knows who you are when you do this type of search. For this reason and many others, it is advisable to use it only with good intentions, or if not, with good protections.

Although some webmasters inadvertently expose sensitive information, this does not mean that it is legal to take advantage of or exploit this information. If you do, you fall into the trendy category of cybercriminals.

Here's a concrete example: not long ago, I was conducting a search for corporate and executive email addresses. I came across the index of a site selling addresses and while digging through the index, I came across a database with 200,000 addresses. Probably because someone had forgotten to associate it with an access code. So I did not commit any breach, but if I used that data, it would be considered theft.

I did two things: made a copy of the database for myself and notified the company that there was a small breach in their security.

Before you read on, be aware that Google will start blocking your connection if you connect from a single static IP. It will ask you to run "captcha" challenges to prevent automated queries as shown below.



This happens very quickly when you make queries that Google finds strange. When you see the captcha above, don't panic. You click, eventually you answer a silly question, and it all starts again. But it's a first warning sign.

The following Google Dorks can be used to detect vulnerable or hacked servers

inurl:/proc/self/cwd

As you can see in the following screenshot, the results of vulnerable servers will appear, along with their exposed directories which can be accessed from your own browser.

It's good to be in your home.

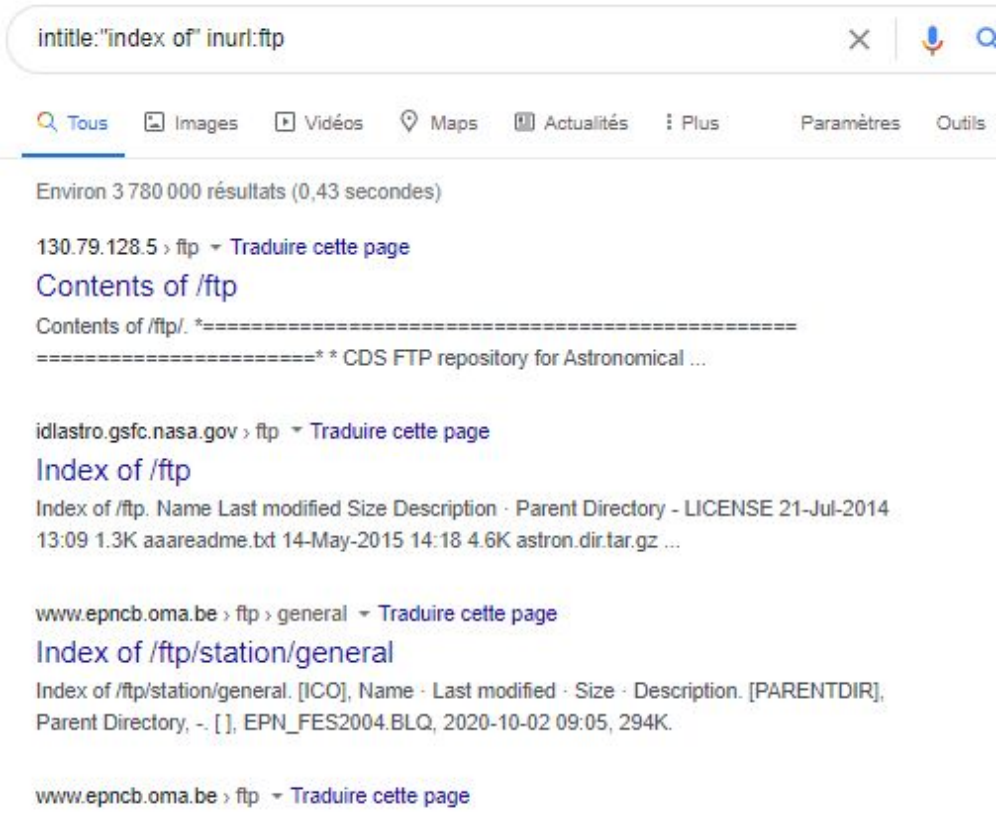
Index of /home/000~ROOT~0(

Name	Last modified	Size	Description
Parent Directory		-	
cache/	2018-10-22 20:59	-	
cpanel/	2020-12-08 12:22	-	
cvs/	2013-11-22 12:29	-	
db/	2019-12-09 09:01	-	
empty/	2016-04-05 18:53	-	
games/	2011-09-23 11:50	-	
installatron/	2020-12-08 08:49	-	
lib/	2020-12-08 11:02	-	
local/	2011-09-23 11:50	-	
lock/	2020-12-08 12:22	-	
log/	2020-12-08 12:22	-	
mail/	2019-05-21 06:38	-	
named/	2020-12-08 08:43	-	
nis/	2011-09-23 11:50	-	
opt/	2011-09-23 11:50	-	
preserve/	2011-09-23 11:50	-	
profiles/	2016-05-10 16:32	-	
run/	2020-12-08 12:22	-	
spool/	2017-10-03 20:28	-	
tmp/	2020-12-08 12:05	-	
www/	2020-12-02 04:41	-	
yp/	2011-09-23 11:50	-	

Google not only indexes HTTP servers, it also indexes open FTP servers. With the following dork, you can explore public FTP servers, which can often reveal interesting things.

intitle: "index of" inurl:ftp

You come across the same kind of index as in the previous case, but in the public sphere.

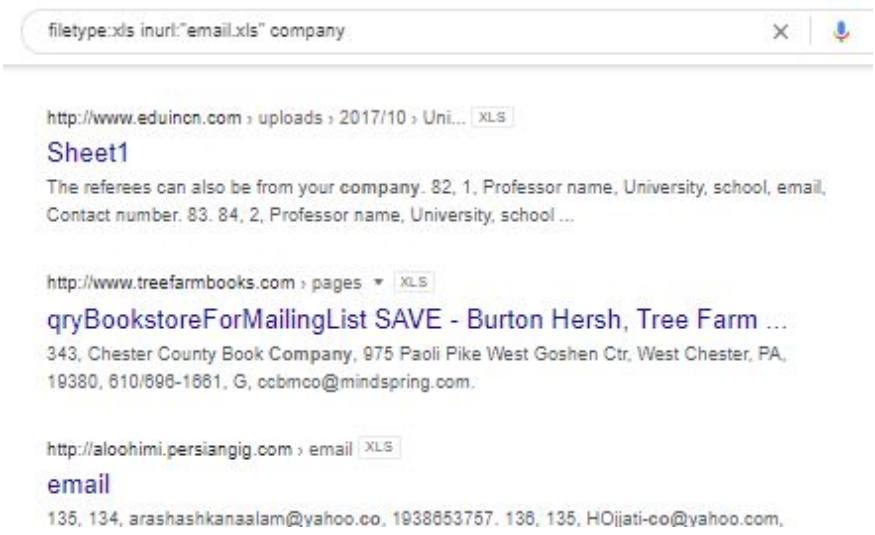


You can see that the second site in the screenshot above is from Nasa. I admit I didn't go in to say hello.

Email lists

It's pretty easy to find email lists using Google Dork. Often, it's neither interesting nor harmful. But when you search for specific databases and find all the emails of students at this or that school or staff at this hospital, it gets trickier. I find hundreds of them without being a geek, but by just applying what is in this chapter. In the following example, we will look for Excel files that may contain emails.

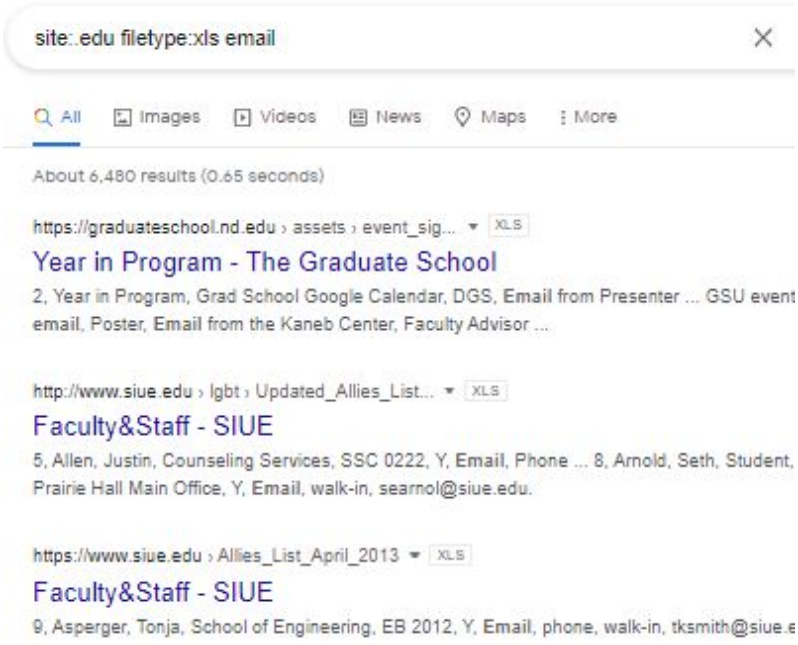
filetype:xls inurl:"email.xls" company



There are lots of possible combinations to find emails. This is just one example among many others.

We filtered to check only .edu domain names and found many students' addresses, with their names of course!

site:.edu filetype:xls email



Remember, the real power of Google Dork comes from the unlimited combinations you can use. My fear with this chapter is that the reader will

apply without looking at the logic. If you master the logic, what you can find in terms of information is limited only by your imagination.

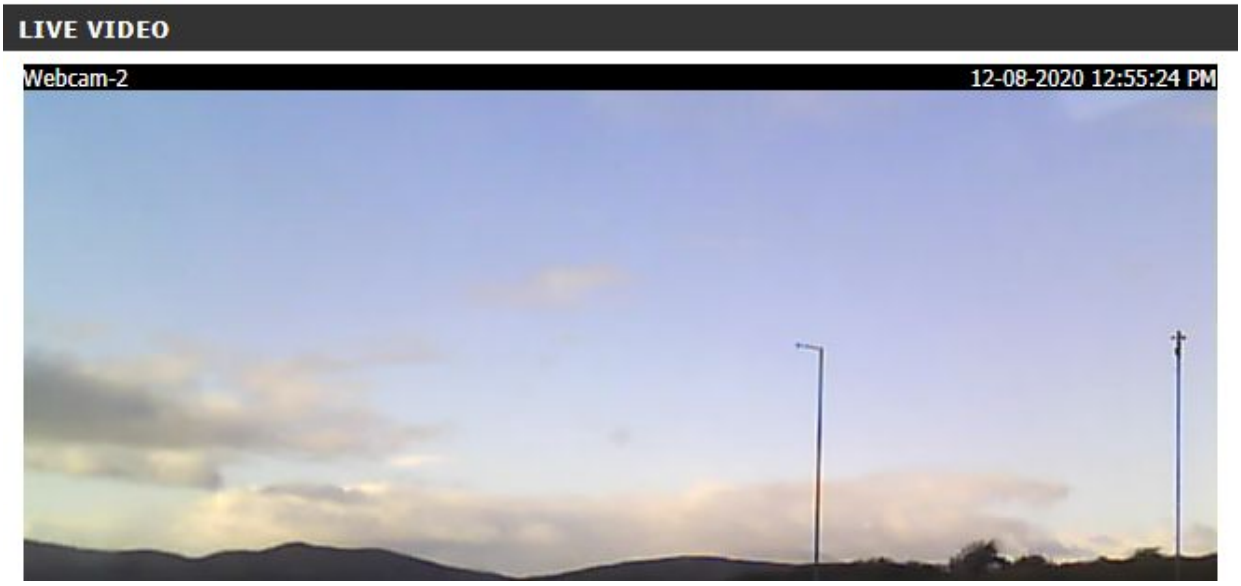
Live cameras

Have you ever wondered if your private camera could be watched not only by you, but by anyone on the Internet?

The following Google hacking techniques can help you to retrieve live camera web pages that, intentionally or not, are accessible without a password.

Here are some tips to access different cameras:

inurl:top.htm inurl:currenttime

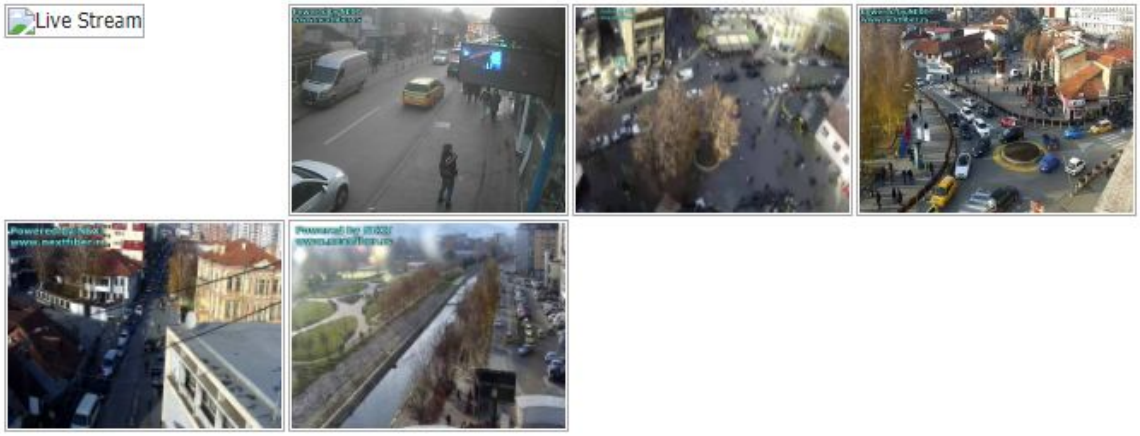


Just as with email addresses, there are hundreds of possible combinations for accessing video cameras.

To find transmissions based on the WebcamXP :

intitle: "webcamXP 5"

This is a public camera from a Polish city. As you can see on the upper right part of the picture, I have not only passive access to the camera. In fact, I have direct access to several cameras in the city, some of them elevated views .



The "multi views" option gives me simultaneous access to various public cameras in the city. Needless to say, we feel safe and another one for general live cameras is :

inurl: "lvappl.htm"

There are many live cameras that can let you watch any part of the world, live. You can find educational, government and even military cameras. On another note, I found a site that maps military sites around the world, with satellite views. Their ambition is not spying, but playing. They have fun.

Where it gets less fun is that these good little guys want to show off their work and anyone can use their favorite hobby for some pretty lethal purposes. if you are creative, you can even do penetration tests on these cameras. You'll be surprised how you can take control of the entire administration panel remotely, and even reconfigure the cameras as you wish. Using these keys, you will often come across webcams voluntarily accessible to everyone, often for tourist purposes. So there is no problem, but when after two minutes, I find myself behind security cameras in the heart of cities or companies. I am both excited by the game, and anxious about the fragility of our information systems.

For your information, here is a list of keys to access public cameras. It's certainly fun and impressive. But keep in mind that it is totally illegal and you will be easily identified. If you take control of a parking lot camera in Alabama, the risk is moderate, just like if you end up in a Nepalese dentist's waiting room. If you access a Siberian nuclear missile site, I'd be less sure how safe you are.

- inurl:ViewerFrame?Mode=
- inurl:ViewerFrame?Mode=Refresh
- inurl:axis-cgi/jpg
- inurl:axis-cgi/mjpg
- inurl:view/indexFrame.shtml
- inurl:view/index.shtml
- inurl:view/view.shtml
- intitle: "live view" intitle:axis
- intitle:liveapplet
- allintitle: "Network Camera NetworkCamera"

You will find at

http://cinemauniversaldownloads.blogspot.com/p/blog-page_16.html an impressive and yet non-exhaustive list of keys allowing you to access cameras. It seems random and with these codes, it is. Nothing prevents you from adding more precise criteria, like a city for example. In this case, we go back to the intention of this book: an active and offensive intelligence tool.

Finally, Camhacker and Insecam are two search engines for unprotected IP cameras. You can search by location, by camera type, by theme etc. and each time, you get a location of the camera with longitude and latitude. We have a

real intelligence tool, accurate and updated. Google hacking codes is great, but you mostly go where you are taken. It's hard to conduct a search on a specific location, whereas with these two sites, it's quite possible. Many of the cameras on these two sites are intentionally public webcams. There is not much to be learned from them. On the other hand, there are also many of these cameras that are city cameras that allow you to have an excellent observation of an area.

https://www.camhacker.com/

http://insecam.org/

The creator of the Insecam.org Project claims to have developed the world's largest online directory of security and surveillance cameras.

The insecam.org website created by an anonymous person is registered with Go Daddy with an IP address that points to Moscow. It streams intercepted images from unsecured webcams/IP cameras of individuals and businesses around the world.

The site is available in English, Chinese and Russian. It references nearly 22,000 cameras worldwide, including 1,077 in France, compared to 5,504 in the United States and 1,746 in Japan.

In total, 26 countries are listed on the site: Spain (284), Germany (529), Turkey (1190), Canada (244), Russia (699). The number may increase or decrease every hour.

The site exposes the privacy of individuals without their permission, which is a clear violation of privacy laws. The addition of IP cameras to the site is likely to be automated by a robot via a complex development that scans all webcams.

The coordinates of the cameras are approximate. They point to the address of the Internet Service Provider and not the physical address of the camera. The coordinates are only provided to locate the city where the camera is located, not the exact location or address.

A little further on, you will find information about the "Shodan" tool that can also help you find cameras.

5. Locating a place or a person with a photo

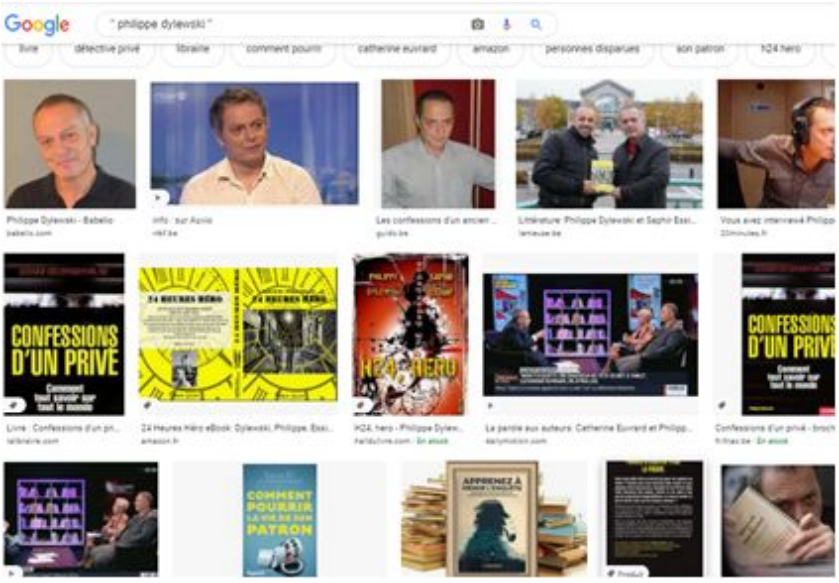
The most complete image search on the Web. That's what GOOGLE says about itself. It was certainly true, maybe it still is, but if you need to investigate an image, Google's monopoly is over.

Google Images is useful in professional information search in many ways, although nothing revolutionary in terms of results should be expected.

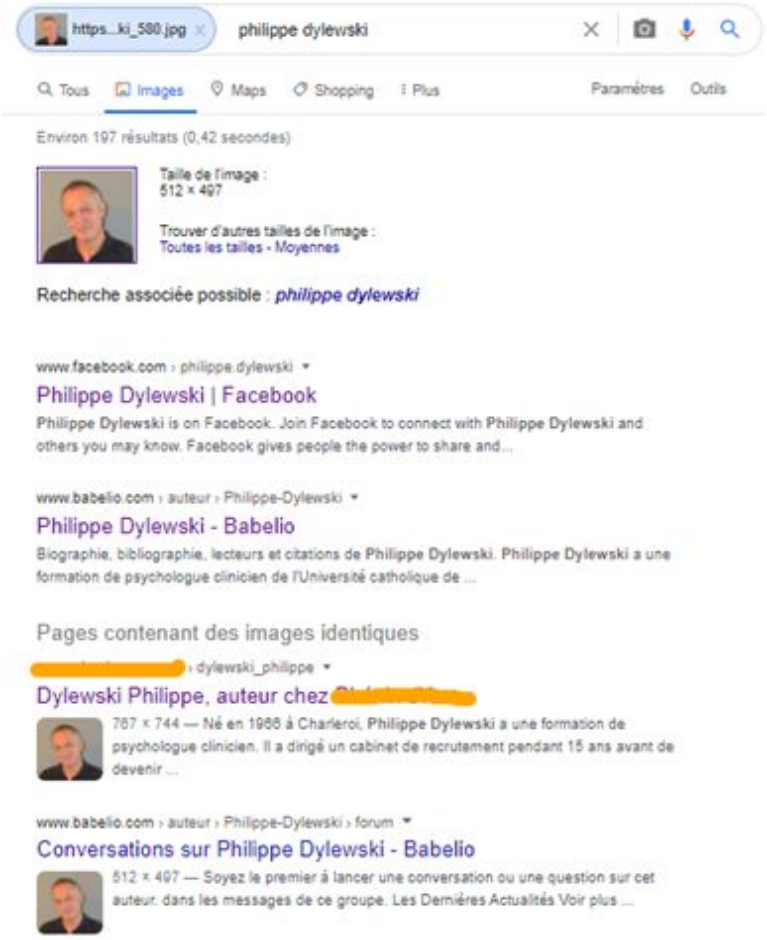
In people search, it's very nice. Type in your target's name (your competitor's manager or one of his salespeople, for example) and you'll have a good chance of seeing his pet reel. If you're really lucky, you'll see that other photos appear. Google searches widely and you will see photos related to your target: people who have your target as friends on Facebook, colleagues, family, etc.

But if you're looking for information about a company or a product, there's a wealth of information here too. Have fun typing "Greenpeace" here and you'll see tons of Greenpeace logos of course, but also adverts, poster campaigns, textbook covers, scanned documents, site photos and flowcharts. Google images also has more advanced applications in the world of intelligence. You can find the origin of an image, at least if it is distributed in several places.

In a moment of megalomaniacal delirium, I conduct a search on myself.



Perfect, I'm reassured, we're talking about me. But suddenly worried, I want to know if these photos have not been published without my knowledge. So I click on the photo I'm interested in until I find myself on the site where it was published, then I point my mouse on the photo, click on the right button of my mouse and click again on "search Google for image".



Its official, I'm not that famous. However, Google Images tracks this photo on 3 sites, including Facebook.

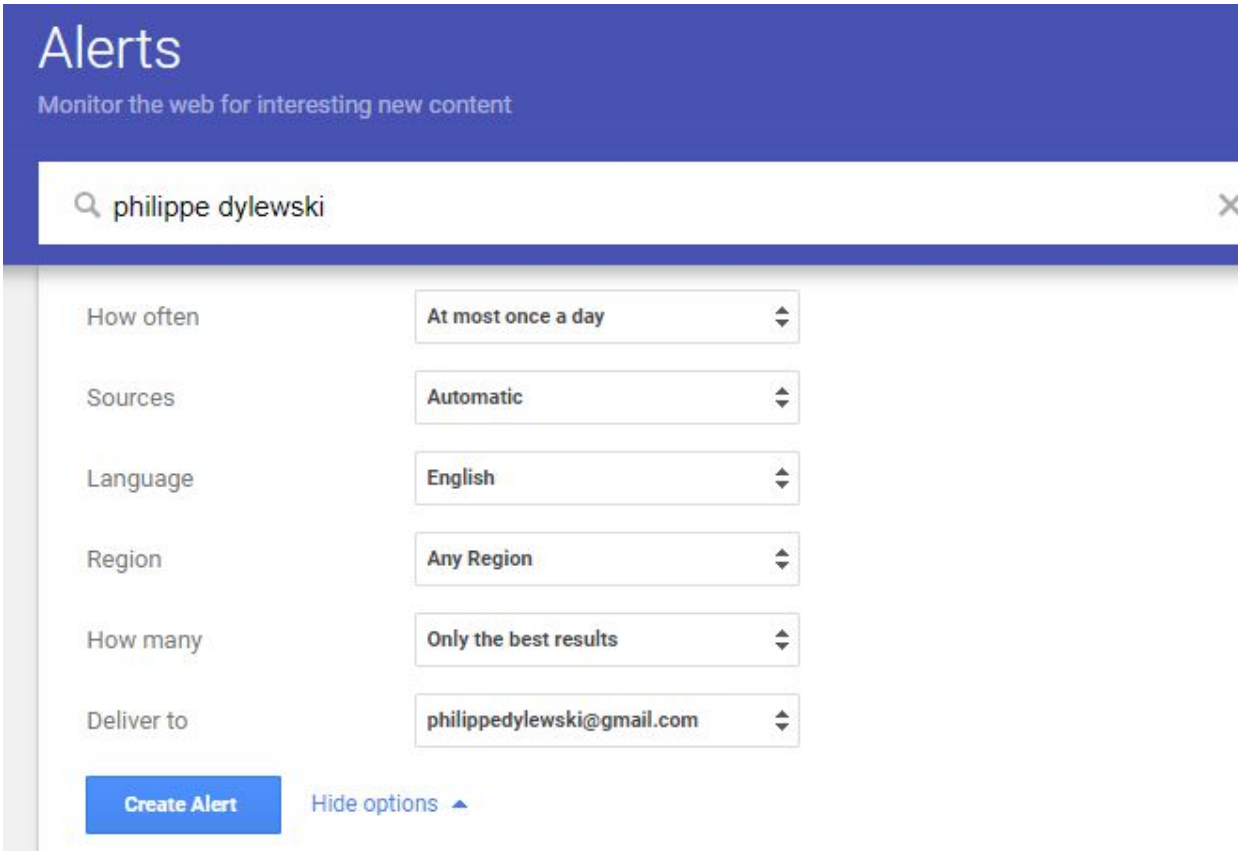
You can also do a search from photos stored on your computer. To do that, you click on the camera at the top right of your page and Google images offers you to download a photo from your files.

You should not expect too many miracles here in the search for missing persons because if the photo in your possession has not been published on a site, you will not get anything at all.

6. Be warned in real time of any change in your target

Google Alert warns you of any change in your target's content, in real time if you want. It's simple, it's free, and it’s efficient. You can launch as many queries as you like.

https://www.google.com/alerts



You can use it to:

- Know what people are saying about you
- Keeping track of what's new with your competitors
- Keep up to date with what is being said about your competitors
- Be informed of any new developments on a topic

My books are often pirated by sites that offer "free" downloads. Almost every time, it's just a scam, but I want to stay informed. With Google Alert, I am notified in real time when a site mentions a book I have written. I decide whether to react or not. But at least I am informed.

For private investigators, the tool can also be useful in the search for a person. If you have searched the planet for your target, without success, you can wait until he or she is in the news. Type in your target's name here, and maybe one day it will work. We agree, the probability is low, but it is still essential to do it. With **Wysigot** , you put your competitor's site on watch and are informed of any changes to their site. As it is an offline browser, you have to download an application.

http://www.wysigot.com

It first sucks up sites, with their scripts, flashes, cookies, etc.

It monitors pages and sites, and alerts you to new information. Wysigot can monitor for you the weather, your mailbox, the stock market, the TV programme, a software update, or the result of a search. As soon as one of these pages changes, it appears in the alarm list and the changes are highlighted in yellow.

7. Google Video

There are lots of video search engines. I've tested a few of them and GOOGLE VIDEO

(https://www.google.com/videohp?hl=en) takes the cake, hands down. This bothers me, because the monopoly is something that bothers me. For my own satisfaction, I can see that in some areas, Google is no longer the best.

Google Video will fetch what you are interested in from a range of video sites: YouTube, Dailymotion, TV channels and others. Again, Google records all your searches.

What's the point of searching for videos on a competitor or partner?

- See the adverts made by the company.
- See reports from TV stations.
- See the films made by the company's detractors
- Visit the facilities.
- Identify key people.

For a spy, this is where the glory is, because you may find videos made by your competitor's employees, hopefully inside the buildings themselves.

But that's not all; Google Videos also offers advanced search options. I'm not going to go on and on for ten pages, but there are some useful features anyway, as you can sort by really relevant criteria like keyword combinations in a classic web search, which allows you to refine when you get too many results.

- Ex: Search by language and country.
- Ex: Duration of the video.
- Ex: Date (although the option is quite limiting).

8. How to find a particular w ord on a web page very quickly?

You are searching a very long article and only one word interests you, (the name of your target for example) or you are looking for a series of numbers in a huge code.

Type "ctrl F" and as in the example below, you will see that the word is immediately detected and highlighted.

This little trick helps you save precious time.

III. The power of OSINT research

When we talk about OSINT (open source intelligence), we may have the feeling that since it is accessible, it is worthless. That for information to be valuable, it must have been found illegally. The principle that what is costly in time, energy or money is valuable.

Information from open sources allows you to find what you need in most cases. Just because information is available, it does not mean that it is easy to find. It is not enough to say that, I will try to convince you of that in this chapter.

US military agencies began using the term OSINT in the late 1980s as they reassessed the nature of information requirements at the tactical levels of the battlefield. Then, in 1992, the Intelligence Reorganization Act determined that the primary objectives of information gathering included key concepts such as

- Intelligence must be objective and unbiased

- Data should be available from both public and non-public sources

Although the concept of OSINT has evolved since then, as it does not include non-public sources anymore, the concept originated at that time.

Open source information (OSINT) is information gathered from public sources such as those available on the Internet, although the term is not strictly limited to the Internet, but rather refers to all publicly available sources.

"OS" (from OSINT) means Open Source. In this case, it is not related to the famous open source movement that offers free access software, but to any publicly available source where the user can obtain the information in his or her intelligence gathering. The key word behind the OSINT concept is information, and more importantly, information that can be obtained for free or almost free. It does not matter if it is in newspapers, blogs, web pages, tweets, social networks, images, podcasts or videos, as long as it is public, free and legal. In reality, none of these criteria are absolute.

With the right information in your hands, you can gain a big advantage over your competitors or speed up investigations into the companies and people you are responsible for. Companies and individuals use OSINT all day long, without consciously knowing it. Sales, marketing and product management teams also use OSINT to increase conversions or simply to be more effective in selling their services to the public.

Whether you are conducting a cybersecurity investigation against a company or individual, or working on the opposite end of the spectrum to identify and mitigate future threats, having OSINT techniques and clear objectives can save you a lot of time.

Most companies do not adopt OSINT to strengthen their defenses against cyber attacks. That's fine, it's convenient. I don't care if it exists out of negligence, ignorance or condescension. The vulnerabilities of our targets are the weapons of intelligence. While there are many OSINT techniques, not all of them will work for your target. First, you will need to ask yourself some questions:

- What am I looking for?

- What is my main research objective?

- Who is my target ?

- How will I conduct my research?

Try to find the answers to these questions, and this will be the first step in your OSINT investigation. Although many OSINT techniques are used by government and military agencies, they can often be applied in the private sector. Some may work, some may not, but that is part of the OSINT strategy - you will need to identify the right sources and those that are not relevant to your research.

1. Risks of conducting an OSINT survey

I divide this concern into three distinct risks:

- **The risk of being detected** : This is the direct contact made using active techniques, or third party services that can get you discovered. If your mission is to collect information about a pool manufacturer on the other side

of the country, being discovered is unlikely to cause you much harm. If you are mapping the American nuclear network in depth for a foreign power, the risk is a little higher and the consequences potentially dramatic for you.

- Risk of losing access to this information: Once they know that you are following in their footsteps or looking for their information, they may start to erase their own traces and close access to public data.

- Risk of becoming the victim: After all, you may end up being the target of an investigation, or worse, the organization you belong to may suffer this fate. Great care should be taken when using active OSINT techniques. Especially if you also use the other strategies suggested in this book.

OSINT is all about tools and techniques. We will look at some of them. There are thousands of them. The first and most powerful of these tools will only be mentioned here. What can be done with Google has already been seen in a previous chapter. This is the case with other tools seen in other chapters, including finding information about your competitors.

I have great confidence in the intelligence of the reader and his or her ability to find what he or she needs.

The last thing we won't talk about in this chapter is dead tools. There are many of them and the OSINT battle kills them every day. Specifically, if I mention a tool in this chapter, it is because it works and I have used it. It is possible that between the time I last used the tool and the time you are reading this chapter, some of the links have died. I have found two ways of dealing with this problem. The first is that if you come across a dead link, would you be so kind as to let me know? The second is that only 100 or 200 copies of this book will be printed at a time, so that it will be constantly updated.

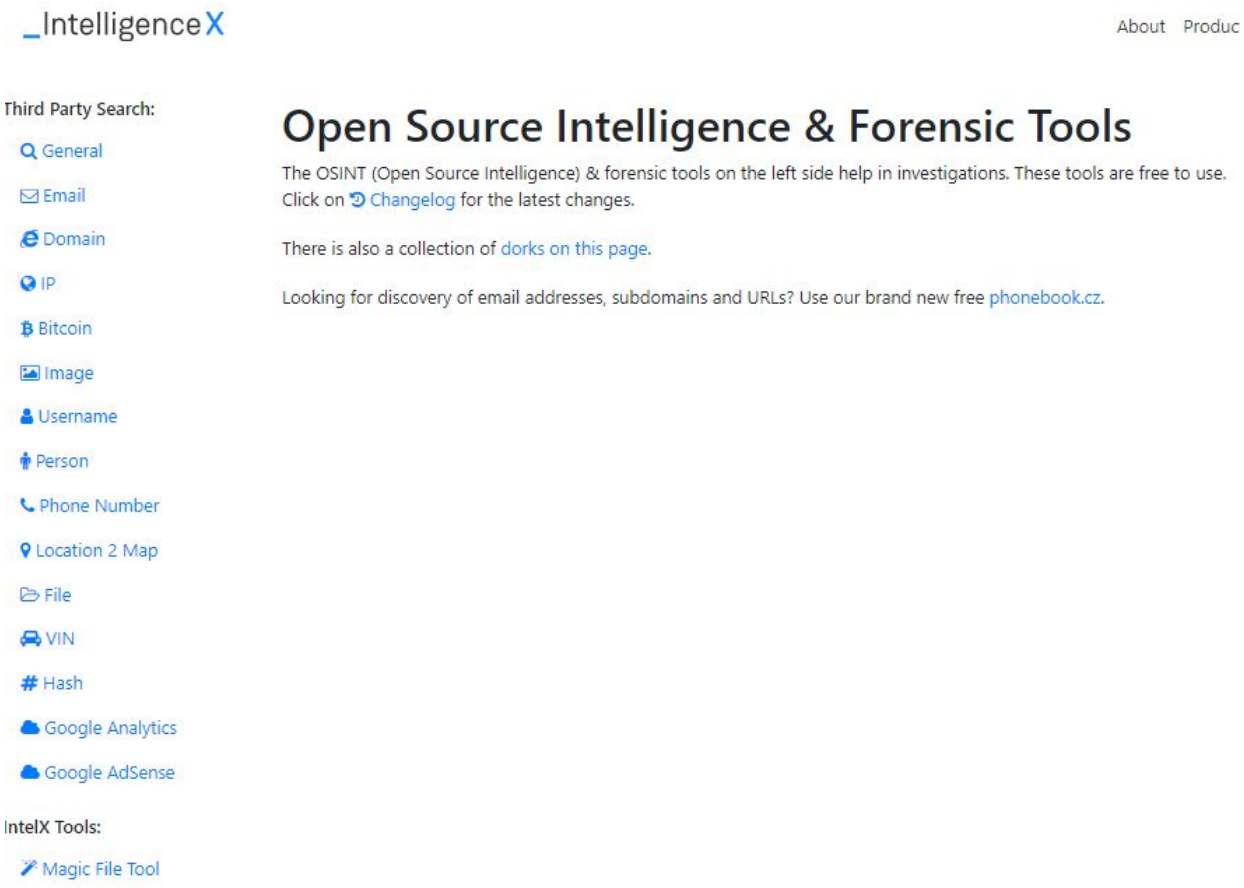
So, here we go:

2. OSINT tools

Although Intelligence X is not a tool to run on your servers, as it is a website, it is a very useful way to get valuable information by searching free search engines, resources and tools available on the Internet. The aim is to provide the best links to useful OSINT data sources. Most of the websites it uses are free, but some may require the payment of a small fee.

Intelligence X is a tree with a thousand branches. It is the mother and father of intelligence. It is the structuring of the great 'whole' of strategic information. It covers dozens of themes, which are themselves subdivided into subgroups, which lead you to an application. We will look at some of them: the most interesting ones, the ones that have not already fallen to the web and also the ones that work in Europe, because many tools are excellent but only work in North America. If you want to test everything, it will take you days but it is exciting.

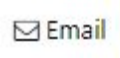
https://intelx.io/tools



As a reminder, when I don't mention a tool in the Intelligence X directory, it's either because it's dead, doesn't give anything terrible, or you have to go through nebulous registration procedures before finally learning that it's not for free . This is because to be a Premium member, you have to pay the modest sum of xxxx dollars.

There is also the case where the tool is both unknown to me and incomprehensible. This will also be your case if you are not a star in computer security.

Here you can search through a whole series of engines. The temptation will be to select all of them in the hope of getting as many results as possible, but this is not efficient because if you select this option, the search will only be done from the first engine checked. You are a good little intelligence soldier and you will conduct your search engine by engine.



You don't waste your time. None of the tools works properly.

We already start with the Phonebook application which finds more than 150 emails belonging to the collaborators of the Belgian newspaper "Le *Soir* ". As I am a nasty spammer, I can say that it is powerful.

I have used it to search for emails belonging to other companies and it is by far the best.

With **Whoxy** , I will know the date of creation of the site but also the other domain names registered. So, if my target has registered .be and .fr companies and forgot to register .com, I can buy these different domain names and use them as I please.

With **Who.is** , I get a lot of information about the technical aspects of the site.

Portscan is a tool for naughty people because it searches for open ports on a server.

OpenLinkProfiler is a link search tool that allows you to check any website's backlinks for free. Just enter the domain name in the search field of the tool and it will start analyzing the website and provide you with a full report of its backlinks. It's free for the moment but it won't last

If you are searching for people in the US, the "person" part will be interesting, for any other country, it's pretty useless. That's it for some X-Intelligence tools. There are so many, check it out, search it, it's so huge.

BuiltWith is an effective way to detect which technologies are used on any website on the Internet. It includes detailed information on the CMS used such as Wordpress, Joomla, Drupal, etc., as well as complete Javascript and CSS libraries such as jquery, bootstrap/foundation, external fonts, type of web server (Nginx, Apache, IIS, etc.), SSL provider and web hosting provider used. BuiltWith also allows you to find out which technologies are currently the most popular or which are becoming trendy. It is without doubt a very good open source monitoring tool to gather all possible technical details about any website. https://builtwith.com/

SpiderFoot is an OSINT automation and recognition tool, which aims to automate the process of gathering information about a given target (IP address, domain name, host name, subnet, ASN, etc.).

You can use it to collect information about any target, such as DNS, Whois, web pages, passive DNS, spam blacklists, file metadata, threat intelligence lists as well as services like SHODAN, HaveIBeenPwned (is your email address compromised?), etc... but you can also try this tool against your own network to see what information you are giving out.

- abuse.ch - Check if a host/domain, IP or network block is malicious according to abuse.ch.
- Base64 - Identify Base64 encoded strings in all content and URLs, often revealing interesting hidden information.
- Blockchain - Query blockchain.info to find the balance of identified bitcoin wallet addresses.
- Cybercrime -tracker.net - Check if a host/domain or IP address is malicious according to cybercrime-tracker.net.
- DNS Raw Records - Retrieves raw DNS records.
- Google Maps - Identifies potential physical addresses and latitude/longitude coordinates.
- HackerTarget.com - Search HackerTarget.com for hosts sharing the same IP address.
- malwaredomainlist.com - Check if a host/domain, IP or network block is malicious according to

malwaredomainlist.com.

In addition SpiderFoot has one big drawback for most readers of this book, however: the results are incomprehensible to the average person. Many automation tools in OSINT require technical skills. If you work in a large company, you will get help from your IT manager. If you are active in a small company, you will have to call in outside help. When this book was first published, ten years ago, internet technology was already well established in the intelligence world, but at a level I could quickly master. This is no longer the case today. Of course, I could learn though It would probably take a few months for me to reach a certain level. So I have chosen to use people who are more competent than I am for the subjects I do not master.
https://www.spiderfoot.net/

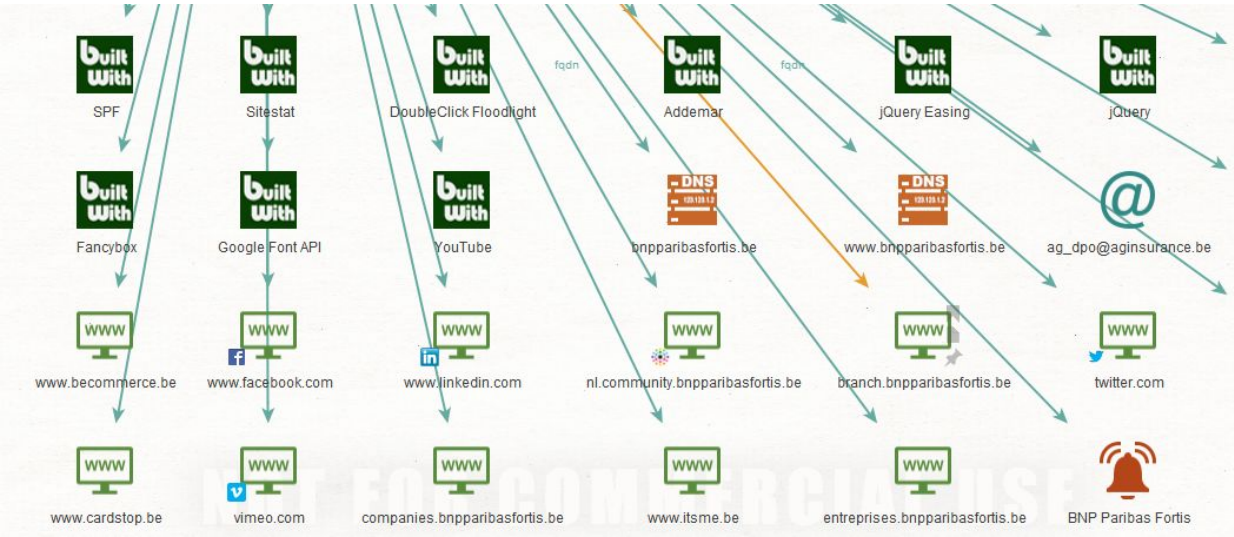
For the intelligence officer who is looking for vulnerabilities in a site, **Spyse** is perfect. It detects vulnerabilities in seconds and you can try it for free.

https://spyse.com/

Maltego is a data mining tool that leverages a variety of open-source data resources and uses the data to create graphs to analyze connections. The graphs allow you to easily make connections between information such as name, organizational structure, domains, documents, etc. Basically, it analyses a large amount of information and then launches a nice graph to help you put the pieces of the puzzle together. Maltego can be used as a

resource at any point in the investigation, but if your target is a domain, it makes sense to start mapping the network with Maltego from the beginning.

You have a free version that is already impressive. It's mostly the visuals that hit home. It really gives you the feeling of being in the middle of something, when you see the existing connections between all the elements of the table.



The other important aspect is that it is a magnificent structuring of information, and each thread of the canvas can be explored further. The software can be downloaded after registration. It is quite easy to learn, but if you try it without a tutorial, you will not understand anything. Well, I didn't understand anything. So after watching two or three videos of a few minutes, I was able to start working.

Some say it is one of the best OSINT tools in the world. It's a tool for business intelligence professionals. If you're the manager of a supermarket and you're suffocating because your competitor is selling his artichokes for 12 cents less than yours, using Maltego is a bit like shooting an ant hill with a bazooka. But if you're a consultant with very fancy clients, your clients will know for sure that you're the new 007 of B2B.
www.maltego.com
I'm kind of like everyone else. I love the underdogs. And I think **Lampyre** is the most underrated of the great investigative tools. To give you a benchmark, when I type in Maltego on Google, I get about 100 times more links than when I do the same thing with Lampyre.

Not only is there little talk about it on the networks, but when there is, it is to say that the site is dead or that its founder is a former FSB (Russian intelligence service). The site is alive and well in September 2021 and if its founder is a former FSB agent, it gives me an excellent reason to be interested in Lampyre.

To access the tool, we are in the classic: a site, a download and free data. The interface of the software is a bit rustic. Getting started is not complicated but watching the tutorials on You Tube will not be a waste of time.

The results are simply amazing.

Using my private email address, Lampyre found my accounts on Aliexpress, Linkedin, Facebook, Amazon, Instagram and Skype.

Using my usual user name, Lampyre found a dozen sites where I am registered.

Using my Belgian phone number, Lampyre found two Skype accounts. As a bonus, the longitude and latitude of the place where I registered... which means my home. The software also found a Snapchat account and another one on Whatsapp.

To test its power, I launched the Facebook Id of someone I know well but who is not among my friends (yes, an ex). Lampyre found two profiles, the place where the person was born and where she studied, although this information is not public on her profile. But also more than 100 profiles liked.

I saw a search conducted on Jennifer Aniston on her Instagram profile. The information is of a high level.

The author of an article on Lampyre says he got chills when he found that Lampyre had found security leaks related to his email address.

In summary, Lampyre is not just an OSINT all-in-one like there are lots of. It accesses information I wouldn't otherwise have. And that's scary.

Like Maltego, the results can be seen as a structured canvas.

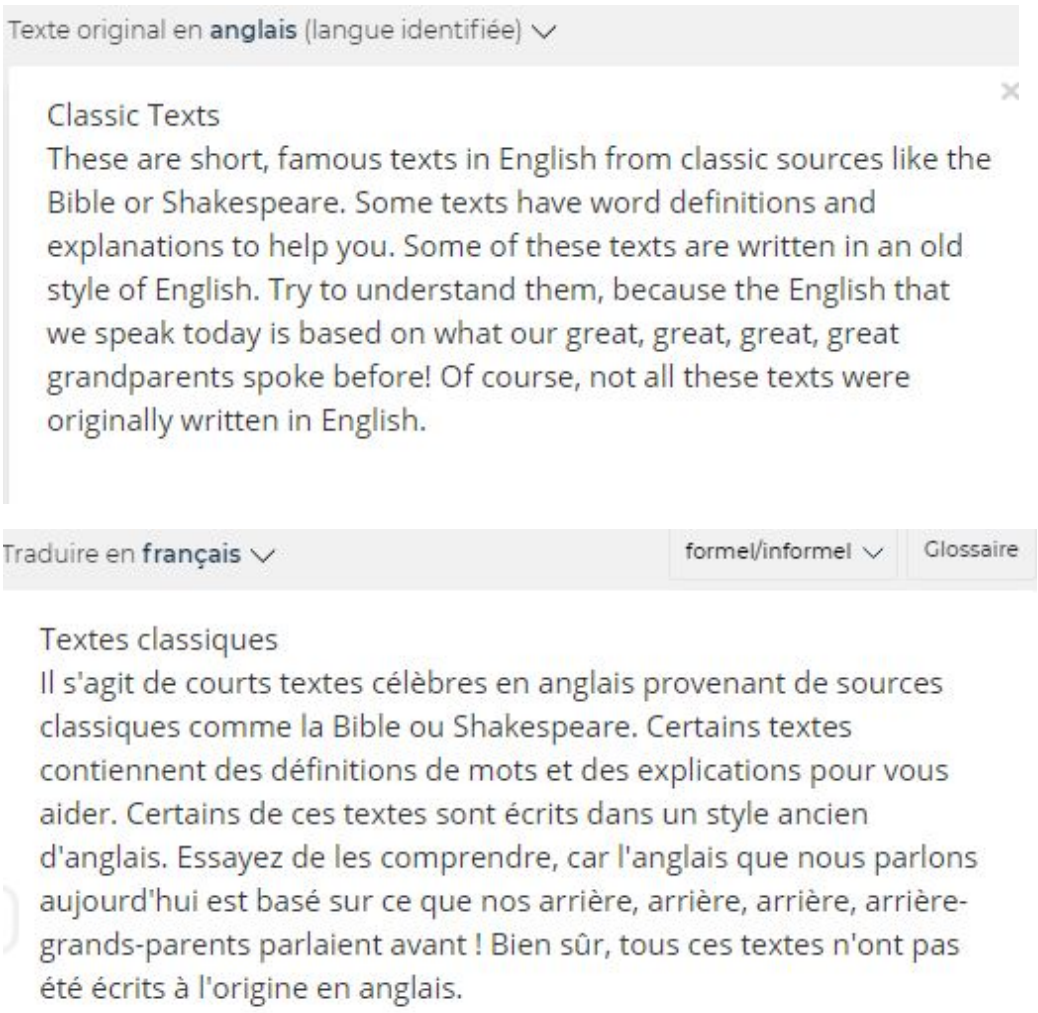
In conclusion, I didn't do my job as an investigator with Lampyre. No due diligence. I run a small organization in the private sector, so it's less important than if you work for your government or a big organization and you have an interest in knowing what's running on your machines. I would strongly suggest that you do so because I don't understand how what seems to be a small organization could create such a powerful tool.
https://lampyre.io/

3. Translate your documents perfectly with artificial intelligence

Until now, translation has been an almost insurmountable problem. Google's translation tool, Google translate, is nice, but it's not very effective. Now there is an absolutely fabulous online translation tool.

DeepL is what you might call an intelligent translator. It takes into account the context. It does not translate literally like other machine translators, but finds the meaning of the text. Is it a perfect translation? Are our graduate translators required to retrain within the hour? No, but we are slowly getting there.

For your investigations in foreign languages, it is absolutely perfect. The language barrier simply does not exist anymore, and if you have to write a document, DeepL is a great help because what you write will be completely understandable to your interlocutor. The tool works with 26 languages. This book is a translation and adaptation of the French edition released in March 2021. At the time, DeepL offered 11 languages. This shows how fast the tool is evolving. As I am involved in searching for missing persons all over the world, I work with private detectives in different countries. I did a test and sent a message to colleagues in 8 different languages. And I asked people how correct the text they sent was in their language. The results ranged from 'very good' to 'no mistakes'. Everyone understood my message, which is the most important thing. Having good translations when you work in OSINT is a big step forward in your work. Below is a text translated from French.



I invite you to compare the two texts. Not to spoil the joy of having found a translator of this level, it is free for texts of no more than 5000 characters, which is still more or less three pages. There is a paid version, which I use, and which costs only a few dollars a month. In truth, I don't really need the paid version, but I pay so much I am satisfied with the tool. Yes, I advertise them, and for free. https://www.deepl.com/

4. The search engine for hackers and the art of entering through doors left open (oops !)

Shodan is a network security monitor and search engine focused on the deep web and the internet of things. It was created in 2009 to track publicly accessible computers within any network.

It is often called the "hacker search engine", as it allows you to find and explore different types of devices connected to a network such as servers, routers, webcams, printers etc....but this will soon also be the case for your toaster, your TV or your air conditioner.

Shodan is pretty much like Google, but instead of showing you images, text, videos and content-rich websites, it will show you things that are more relevant to the interest of computer security researchers, such as SSH, FTP, SNMP, Telnet, RTSP, IMAP and HTTP server banners and public information.

The results will be presented in order of country, operating system, network and ports.

Shodan users are not only able to access servers, webcams and routers. It can be used to scan almost anything that is connected to the internet. Look at your home or around you at what is connected and shudder.

You could say that Shodan is the perfect tool for the geek and only for the geek. Who spends his nights looking for security holes in a network? That's true. But it is also a powerful tool for an investigator who now has access to all the connectivity of a target. But the grail is for the marketer which is a bit more unexpected.

Connected devices display their brands and model numbers directly on the login pages and in the http headers. From there, one could imagine Shodan detecting the makes and models of your growing number of connected devices. I'll leave you to imagine the rest.

As a tool, Shodan is pretty easy to pick up. After all, it's just a search engine. From the "explore" function at the top of the screen, you can quickly understand how the tool works. But if you are not a net afficionado, it is the interpretation of the results that will be problematic.

The question of the legality of Shodan arises. Yes, Shodan is legal. After all, all it does is to find flaws and compile them. What other methods could do whereas Shodan may fall into illegality is what you do with it.

The price: if you do a one-off search, access to Shodan is free. As soon as you want to use it as a more sophisticated and regular search tool, you will have to pay. Starting at 59 dollars per month.

https://www.shodan.io/

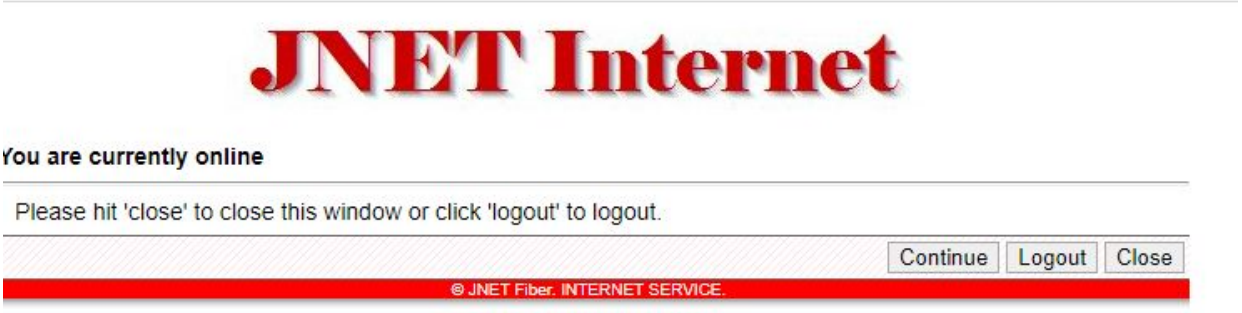
Angry IP scanner is a fast and user-friendly network scanner for Windows, Linux and Mac. It is very extensible, which allows it to be used for a wide variety of purposes, the primary goal being to be useful to network administrators. This is the official version. It is port scanning software used to scan for the presence of computer devices connected to a network. It's great for monitoring your own computer security as it detects weak points in your network in no time. But it's especially nice to see if certain ports are open on your neighbor's or whoever's network you want, as soon as you know their IP address, which is very easy.

https://angryip.org/

I can run angryip from an IP address that I encode and it will look for open ports around that address.

192.168.2.241	[n/a]	[n/s]	[n/s]
192.168.2.242	[n/a]	[n/s]	[n/s]
192.168.2.243	[n/a]	[n/s]	[n/s]
192.168.2.244	[n/a]	[n/s]	[n/s]
192.168.2.245	[n/a]	[n/s]	[n/s]
192.168.2.246	[n/a]	[n/s]	[n/s]
192.168.2.247	[n/a]	[n/s]	[n/s]
192.168.2.248	[n/a]	[n/s]	[n/s]
192.168.2.249	[n/a]	[n/s]	[n/s]
192.168.2.250	[n/a]	[n/s]	[n/s]
192.168.2.251	[n/a]	[n/s]	[n/s]
192.168.2.252	[n/a]	[n/s]	[n/s]
192.168.2.253	[n/a]	[n/s]	[n/s]
192.168.2.254	4 ms	login.ibsg.nvk	80,443

When the little green light comes on, it means that I have found an open port. I copy/paste the IP address in question and send it to the search bar. And I get the confirmation of the internet subscription of the building where I live.



But that's a bit of a fluke. If I do the same thing with the IP of a particular site, I might find some open ports. Which MAY lead me to something. And that something will probably ask me for a login. A camera, a scanner, a printer, anything that is potentially connected. Normally, during installation, the person in charge is supposed to create a password and a login. Sometimes the person does this, sometimes they just say "administrator" or "admin" or sometimes they leave the default credentials of the machine.

There are thousands of them, depending on the brand and the device.

www.routerpasswords.com/ is a database that will list most of the default passwords of every connected device imaginable. Again, this site only provides significant information because people are careless. But everyone is careless at any one time or the other.

Manufacturer	Model	Protocol	Username	Password
AXIS	NETCAM	TELNET	root	pass
AXIS	ALL AXIS PRINTSERVER	MULTI	root	pass
AXIS	WEBCAMS	HTTP	root	pass
AXIS	540/542 PRINT SERVER	MULTI	root	pass
AXIS	NETCAM		root	pass
AXIS	2100	MULTI	n/a	(none)

In the example above, for the AXIS security camera brand, we have the default username and password for the various models.

5. Locating an IP address

An IP address (with IP standing for Internet Protocol) is the number that identifies each computer connected to the Internet, or more generally and precisely, the network interface of any computer equipment (router, printer) connected to a computer network using the Internet Protocol (Wikipedia definition).

There are different types of IP addresses such as private IP addresses, public IP addresses, static IP addresses and dynamic IP addresses.

Private IP address

A private IP address is the address of your connected device on the home or office network. If you have several different devices connected to a single Internet Service Provider (ISP), all your devices will have a unique private IP address. This IP address is not accessible from devices outside your home or office network.

You can find the private IP address of your device using a few techniques. If you are a Windows user, simply go to the command prompt and enter the command ipconfig. If you are a Mac user, then you need to enter the following command ifconfig in your Terminal application

If you are using the internet on a mobile phone, you can go into your WiFi settings to find the IP address. iOS users can find the IP address by clicking on the "i" button next to the network they are connected to. Android users can click on the network name in their Wifi settings, and the IP address will be displayed.

Public IP address . Your public IP address is the primary IP address that your home or business network is connected to. This IP address connects you to the world, and is unique for all users.

Static and dynamic IP addresses . All private and public IP addresses can be static or dynamic. IP addresses that you manually configure and attach to your device's network are called static IP addresses. Static IP addresses cannot change automatically.

Dynamic IP address is automatically configured and assigns an IP address to your network when you configure the router with the Internet.

Once you have the IP address of a site or person, you can find an approximate location.

I use https://www.iplocation.net/ . not because it is better than any other, but because it compares the results of several IP address search engines. In my case, two of the four engines locate me in Thailand, in the province of Chonburi and more precisely in Pattaya, where I live at the moment.

IP Address Details

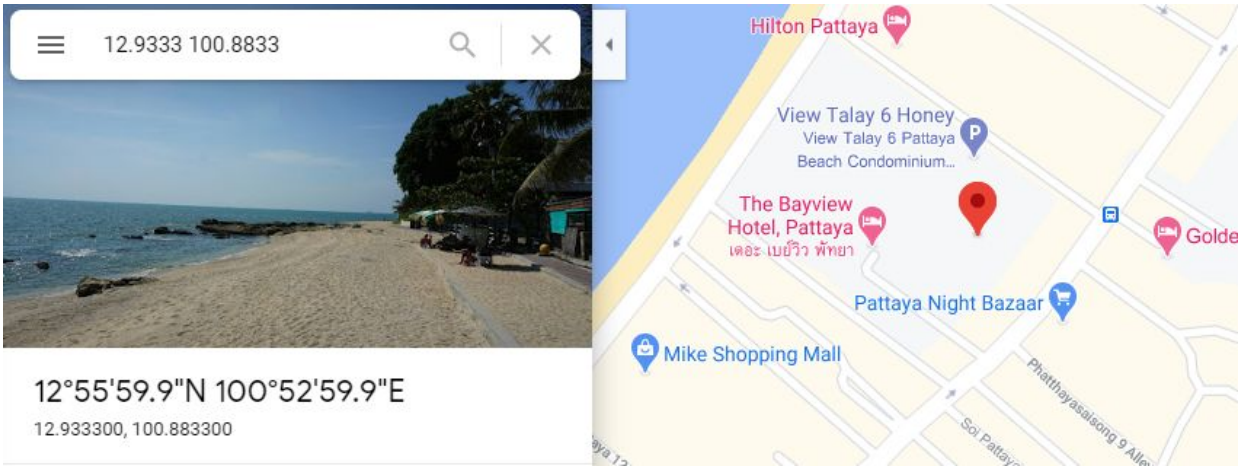
IPv4 Address	**183.89.0.64** **Hide my IP with VPN**
IPv6 Address	**Not detected**
IP Location	Chon Buri, Chon Buri (TH) [Details]
Host Name	mx-ll-183.89.0-64.dynamic.3bb.co.th
ISP	Triple T Internet PCL
Proxy	No proxy present
Platform	Windows 10
Browser	Chrome 92.0.4515.159
User Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36
Screen Size	1366px X 768px
Cookie	Enabled
Javascript	Enabled

The engines give me a latitude and longitude which I enter into Google maps. https://maps.google.com/

It's not like in a movie where the terrible machine of the overpowered agent finds my flat number. This is because I don't live where Google maps locates me but about 500 meters away.

Locating the IP of a website is even more tedious because the website can be hosted anywhere and rarely where the company or organization is located. I have a site hosted at one.com and when I locate the IP of my company, I am located in Scandinavia.

But as with any investigative method, this one is worth trying, because it can yield interesting results.



As you know, your activities on the net are monitored, unless you use a search engine like Duckduckgo or are protected by a VPN. Getting a person's IP address is not only a way to locate that person approximately, but you can, for example, find out what the person has been downloading lately. This is what https://iknowwhatyoudownload.com/ does and it does it very well.

Torrent downloads and distributions for IP 183.89.119.122

Asia | Thailand | 3BB Broadband

183.89.119.122 is your IP address.

Computers connected to a network are assigned a unique number known as IP Address. IP addresses consist of four numbers in either a permanent (static) IP address, or one that is dynamically assigned/leased to it.

Use internet connection of other people (Wi Fi, their computers, tablets and smartphones) to know what the or see other similar IPs: 183.89.119.105 183.89.119.114 183.89.119.115 **183.89.119.122** 183.89.119.123 18 183.89.119.138

FIRST SEEN (UTC)	LAST SEEN (UTC)	CATEGORY	TITLE
Sep 16, 2021, 1:24:48 PM	Sep 16, 2021, 1:24:48 PM	Movies	Godfather of Harlem
Sep 16, 2021, 12:31:28 PM	Sep 16, 2021, 12:31:28 PM	Movies	Soorarai Pottru
Sep 16, 2021, 12:30:04 PM	Sep 16, 2021, 12:30:04 PM	Movies	Dveselu putenis
Sep 16, 2021, 12:23:51 PM	Sep 16, 2021, 12:23:51 PM	Movies	Unknown Battle
Sep 16, 2021, 12:22:44 PM	Sep 16, 2021, 12:22:44 PM		[OxTorrent.nz] Gagarin
Sep 16, 2021, 12:16:18 PM	Sep 16, 2021, 12:16:18 PM	Movies	Young Royals
Sep 16, 2021, 11:42:33 AM	Sep 16, 2021, 11:42:33 AM	Movies	Boss Level

6. Locating an email address

To trace an email, you need to locate the header of the email that accompanied it. Every email has a header and a body. An email may go through several stages and a header is added with the IP address of the mail server that processes the email. When an e-mail reaches its final destination, your e-mail provider adds its IP address to the header. The IP address of the very first header added to the email is the IP address of the sender's email server.

What is an email header?

The header of an e-mail contains information about the e-mail such as the sender, recipient(s), subject, date/time of arrival, attachments and the path of the e-mail from sender to recipient. Not all emails have a proper email header that allows you to trace the email back to the original sender.

Where is the email header?

To send and receive emails, we use email clients such as **Outlook** and **Thunderbird** . With the proliferation of free email providers, many of us use the webmail interface provided by **Gmai** l, **Yahoo** and **Hotmail** . Each webmail client and interface offers different ways to retrieve an email header.

Gmail web client

Open the email message whose header you want to locate. Click the down arrow next to the Reply link on the right side.

Select View Original to open a pop-up window with the header and body text.

```
Delivered-To: philippedylewski@gmail.com
Received: by 2002:a54:2091:0:0:0:0:0 with SMTP id v17csp509238ecn;
        Thu, 19 Nov 2020 10:23:28 -0800 (PST)
X-Google-Smtp-Source: ABdhPJzR0hMvxDmUGEO23ckQ7rMT/QJqRrxma4Yx+Xxn3PoMyrbrkVY08D2Ep/JYUy3d2uhWrOTw
X-Received: by 2002:aa7:d443:: with SMTP id q3mr33715137edr.262.1605810208675;
        Thu, 19 Nov 2020 10:23:28 -0800 (PST)
ARC-Seal: i=1; a=rsa-sha256; t=1605810208; cv=none;
        d=google.com; s=arc-20160816;
        b=I4oL3ZHXv3zL0732Lz2bBGtsapgntOVSYSO9DBXC7bfzFBPmSGZqhTXY4TlSeu9FuE
         qhIwwO4N6eYdLYF+oJzZyplHlyS1rqxGBXgj20K0x+o0XhSqkHmFyQbTEJkwNhCvChL8
         CGLAV4ijAMk9iWfZeFupPIqqc5KmdRaPEarUoddkIIlQbEdqBHxSgPj2irlMmnFEl1ps
         oFOyW5dbjmLCNuDRYiKeYMiGBYvs07HUvDK20rIq0pn5Xk28xCU0KsllprdGUUq6D+Mc
         9JqzFlsFuJG5sEZSuJBsiGfze/9WqPUr8isSROKbui0Dtqzo53EXfFDtwRQJNEuQnk30
         gAzQ==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=subject:message-id:date:thread-index:mime-version:in-reply-to
```

Yahoo Web Client

Open the email message for which you want to locate the email header.

Click the down arrow next to the “more” link.

Select View Full Header to open a popup window with the full header.

Outlook Webmail Client

Open the email message whose header you want to locate.

Click the three dots (...) next to the Forward link on the right hand side.

Select View Message Details to open a pop-up window with the complete header.

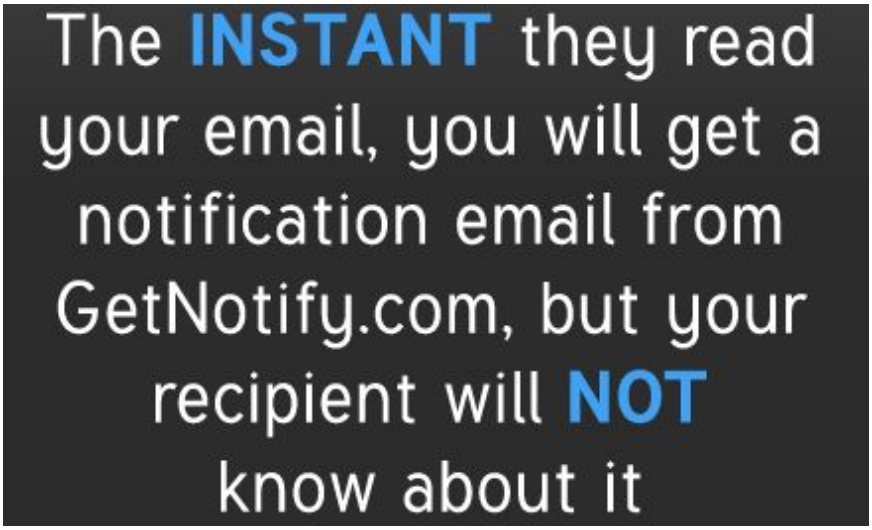
Be aware that a message sent with a Gmail address is not traceable via its IP address.

If you're not too keen on parsing every line of a header to find out the IP address, there is a tool that will do this much faster than you. http://mxtoolbox.com/EmailHeaders.aspx

With https://emailrep.io/ you will know if an email address has a bad reputation, if it has been used massively to send spam, or if the address is blacklisted on certain servers and since when.

https://validateemailaddress.org/ validate s the existence of an email address free of charge, simply connects to the mail server to ascertain the validity of the email address, verifying whether the email address and username are properly formatted and actually exist. This little tool won't tell you if a mailbox is being accessed, but it will at least tell you if the address is alive.

https://www.getnotify.com/ allows you to send a message by email and to know very precisely when the message has been opened. For an investigator this is obviously a very important tool, especially as the person who opens the message will not know that you have this information.



http://www.mailtracking.com/ does exactly the same job.

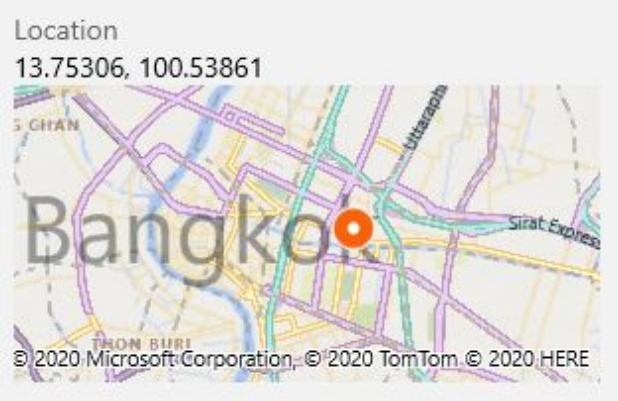
7. Finding information about the origin of a digital photo

Smartphones (and many digital cameras) embed GPS coordinates in every photo they take. The photos you take contain location data, at least by default.

The GPS coordinates are stored as "metadata" embedded in the photo files themselves. All you have to do is look at the file properties and search for it.

In Windows, you right-click on a photo file, select "Properties", and then click on the "Details" tab in the properties window. Look for the latitude and longitude coordinates under GPS.


Madam
VILAI
Made to order



I took this photo on a small street in Bangkok on 11 November 2020. My phone's features, I now know, are enabled by default. This means that the GPS coordinates of the shot have been recorded. W hen I say 'recorded', it's not just about it for when I zoom in on the map, I get straight to the street in question.

You will also have other less important information, such as the make and model of the camera, the date the picture was taken, the angle, the exposure time, the picture taken with or without flash etc. which is wonderful for an intelligence mission: if you have access to the original photo and not a copy and if the person has not deactivated the default recording of GPS coordinates. As for photos found on social networks, you will not be able to locate them as most networks block the publication of photo metadata.

8. Tracing an in dividual's life through a photo

Facial recognition and identification of people for the general public is no longer a dream, or a nightmare depending on personal views. The technology exists, you've seen it in lots of films. You tell yourself that it's reserved for government agencies to locate evil terrorists. That was true until recently. There's a simple rule with intelligence tools, and this rule is probably true in other areas: any advanced technology that is reserved for security and intelligence services will end up in your supermarket at some point. If a technology exists and people are interested in it, it will end up in the public space. Because if one person invented it, another person will succeed to do the same. A third person will produce it less expensive.

A technological advantage is always short-lived. Facial recognition is no exception to this rule, as we will see in this chapter. There are many other

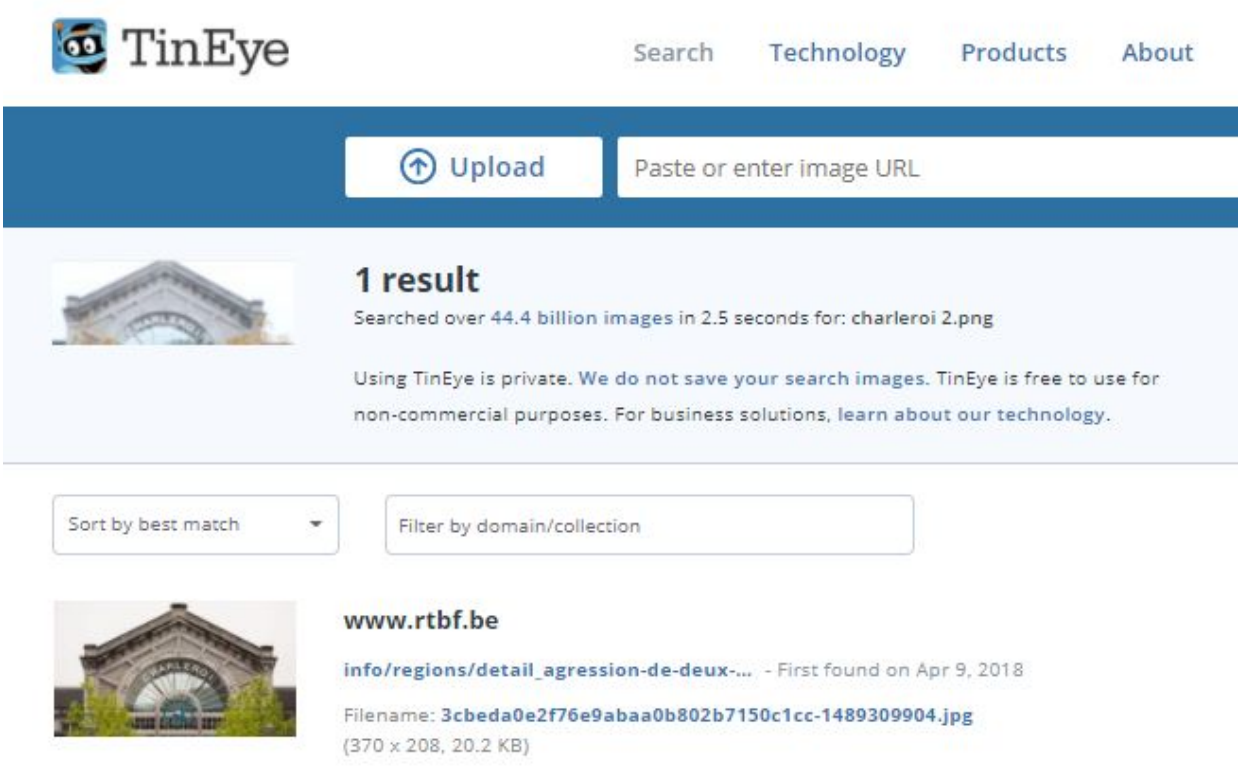
ways of tracing a photo and obtaining information from it. It takes method, hard work, imagination and a little luck.

This photo was taken to promote a book written with my partner and friend. It is in Charleroi, Belgium. It was published in a newspaper, so if I run it through Google Images, no problem, I can locate the photo.

But let's imagine for a moment that it's not a public photo. So I took a screenshot of the background, where you see a building.

This is a simple, low-quality screenshot.

I run it through **Google Images, Bing, Yandex, and TinEye.**



TinEye's original purpose was to find other sizes of the same image, and for many years that was all they provided. They now claim to have a database of two billion images and are adding ten million per month. TinEye focuses entirely on finding other uses for the same image. My screenshot is located, without the link being a photo identical.

The engine simply recognized the building what Google and no other engine could do.

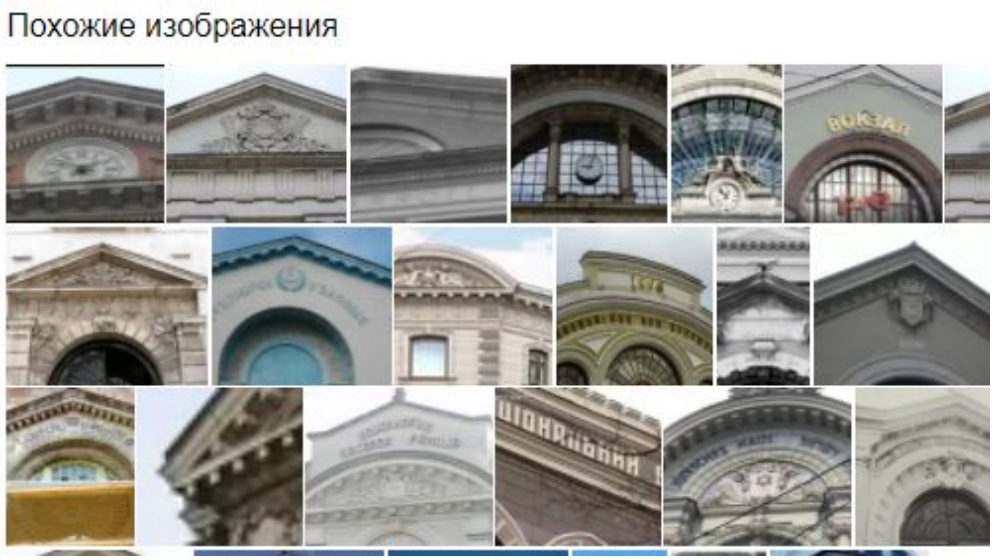
On the other hand, when I run the original photo on Tineye, the engine does not identify it. In other words, locating a photo can be done in a simple way if it is in the public domain. If it is not, it is up to you to look for a detail of the photo, enlarge it and launch it on the various sites we have just mentioned.

Google Images, Bing, Yandex and Tineye each have their own special features in relation to reverse image search.

Google does its best to identify what an image is about, not who. Often, when you do a reverse search for photos with Google, it will return answers like "man" or "girl". The results are usually divided into three sections:

A few search results for what the algorithm thinks is the photo, visually similar (but not identical) results and pages that contain identical images. The search is also limited to a single topic. So if you enter a photo of a house near a lake with mountains, you won't get photos of houses near a lake with mountains, only visually similar houses, regardless of lakes or mountains.

Yandex is a goldmine for searching for inverted images. It provides additional sizes of the same image, visually similar images, and many results where similar images appear on the pages. In our example with Charleroi station, it failed to identify the location precisely, but offered me many very similar locations getting closer and closer.



https://yandex.com/images/

Bing has a unique feature that I really like: you can crop out areas of your photo and see the results live. This is great for high quality images with lots of identifiable subjects. Also, compared to Google, Bing tries to identify elements in a photo and find images that contain all those elements. For example, a photo of a vintage car parked next to a tree will trigger matches that contain a tree and a vintage car, whereas Google chooses a single strong subject and follows it. Bing also distinguishes itself by proactively trying to identify faces, products and other elements in images. A high-resolution image of several famous subjects will highlight each of them. In the case of Charleroi station with a bad picture, Bing finds nothing. However, when I use a good quality photo of a public building, it works very well.

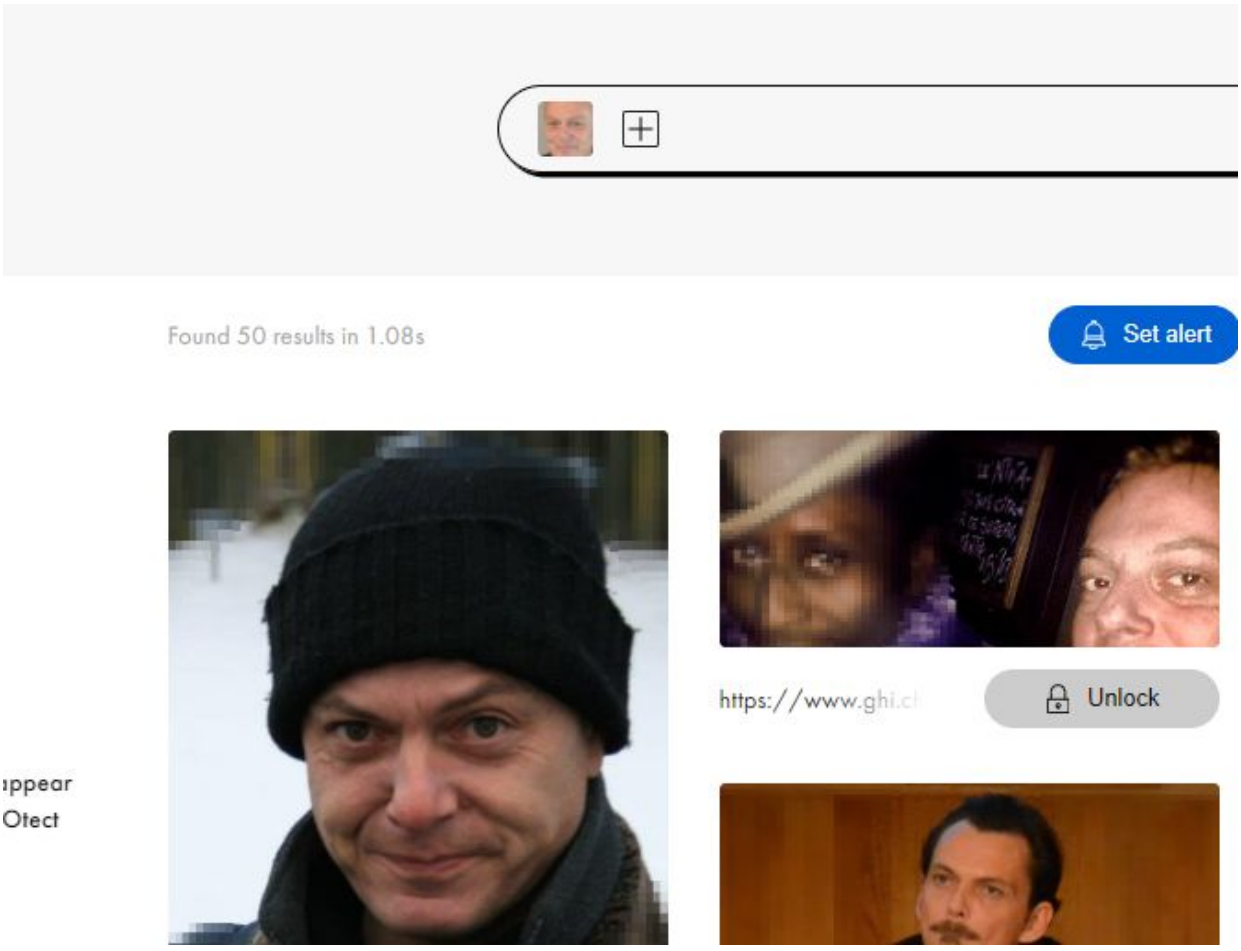
https://www.bing.com/images

A Polish site is completely different from anything else. With **Pimeyes** , we are entering science fiction or rather into facial recognition. It is no longer a question of finding the same photo in different places. It's about finding photos of the same person.

In the example below, I ran a photo of myself taken in 2018 through the engine. A few seconds later, the site offers me a whole series of other photos. One of them is a photo of mine taken on holiday in Scotland in 2008. The other photos offered are not mine, but often very similar. On one of them, I have doubts whether it is really mine or not.

Another such application exists in Russia: **Findface** . It has been used in Moscow's security cameras since 2020 and is able to identify just about anyone through the use of Russia's largest social network. When it comes to absolute lack of privacy, it's going to be hard to top, but I'm sure we'll get there.

Pimeyes also allows you to submit multiple photos of the person you are looking for so that the software can send you a notification when new photos are posted online.



The tool is not perfect. It requires a front-facing photo, taken from fairly close range but it opens the door. The moment when it will be enough to take a photo of a person on the street to identify them on social networks, we will be nearly there.

Free tests can be done, but the links to the photos are hidden. The subscription starts at 15 euros per month.
https://pimeyes.com/
A commercial application of reverse image search was requested by a client who was looking for the manufacturer of a cosmetic product. The customer knew that the product was made in Asia and wanted to import it to Europe. The name of the product was different from one country to another, which made it difficult to trace the source. When I Googled the name of the product, I found lots of distributors, but not the manufacturer. Most distributors, regardless of the product, don't make the promotional photos themselves for marketing. Most often they use the manufacturer's photos. So

I searched with some photos from distributors and found the Thai producer in a few minutes.

As you can see, each search engine has its strengths and weaknesses. Also remember that none of these search engines deeply indexes Instagram, Twitter, Facebook and other social media. It is important to use all of these search engines when conducting a survey, as you are likely to miss a correlation if you do not.

Reverse photo searching is a major focus of investigation. For a journalist, it allows you to verify that a photo is not used as part of a fake.

Is the photo supposedly taken during a riot genuine?

Is it the same riot? On the date we are talking about? Could it be an event that took place elsewhere?

For the thorough investigator, this is a great tool in the search for a person.

9. Advanced investigations via satellite images

For an investigator, **Google earth** or **Google maps** are indispensable tools today. **Google maps** is a detailed mapping system and Google earth contains extremely accurate 3D data, allowing you to explore the streets of any city in the world.

In Google Maps, you can find photos by clicking on the "Photos" section under the map search bar on the left side of your screen.

Google Street View is located in Google Maps. It contains detailed 360 degree photographs taken at ground level and linked together. This allows the user to literally walk the streets and identify buildings, businesses, monuments etc with relative accuracy. Note that you can't read the names at the entrance of a building; for that, you'll still have to move around.

If you need to prepare a stakeout, you have access to the whole neighborhood, via maps or satellite images, which allows you to prepare your observation. Often, you have the possibility to go for a walk in the district thanks to the "street view" application which is very useful when you have to.

If you are doing an audit of a business and you find that the address you have is a post office address, a dilapidated building or a vacant lot.

If your job is to secure a location, such as a stadium, you will have an aerial view of the stadium, mapping of the entire area and also a wealth of photos of the stadium, both inside and out.

If your job is to gather information about a company, you can get a close-up aerial view with a bird's eye view of the facilities.

The bad news for would be terrorists is that most "secret defense" sites are blurred. This can be compensated for via **Google's video** function. Indeed, if I pass over the Heysham Nuclear Power Station (UK), the satellite function of Google map will not work because the terrain is blurred. But if I type the words 'Heysham nuclear' into Google video, I end up with a lot of film material. Taken separately, these films do not represent a safety hazard. It is the number of films and the diversity of the images that will be a safety hazard.

If I type the same words into Google images, I will find thousands of photos taken inside or outside the plant. It's simply frightening.

Films, videos, maps and satellite images are totally complementary tools and you will get the same kind of results with lots of supposedly confidential places. You can use Google earth without downloading it, but you will miss out on a lot of features. Since it's free and great, I urge you to download it here:
https://www.google.com/earth/
Google Earth offers a number of features that Google Maps does not, including historical satellite imagery and 3D models of terrain and buildings. It is also possible to enter some public buildings.

Waze is a live traffic and navigation app that works for GPS-enabled mobiles and tablets (Android and iOS). Basically, it's a GPS, only better, except for the adverts that pop up regularly. The advantages of Waze, apart from being free, are that you can search for a place based on its address or its name. As the information arrives in real time, you will know when to change your route according to road works or accidents. Waze also warns you of speed cameras and static police forces.

https://play.google.com/store/apps/details?id=com.waze&hl=fr&gl=US

Yandex Street View is like Google Street View, but is not as good unless you have to investigate in Russia, Ukraine or Turkey. In that case, the results will be better since you can move around in 360 degree photos and on a map at the same time. It is very useful for anticipating a visit. https://yandex.com/maps

Bing maps does the same thing as the Google series, except that here we are at Microsoft and the same technology is not used. This is already an advantage, because different technology means different results, even if it's just different photos from the same site. When one doesn't satisfy, you move on to the other. Bing maps has a particular feature that can be useful: real-time traffic information. https://www.bing.com/maps

Wikimapia is a handy open source mapping platform for analyzing satellite imagery because it integrates imagery from several providers (including Google, Bing and Yahoo) and allows you to switch between them. You can quickly switch from one set of images to another to see how the same place looks elsewhere. Although it is a private company, it is a collaborative platform because each user has the opportunity to enrich the experience of others. https://wikimapia.org/

Zoom Earth - Near real-time satellite data and high resolution archival data. Fairly similar to Google Earth (especially since it's the Bing competitor), Zoom Earth shows the most recent satellite images and aerial views in a fast, zoomable map. The platform pulls in refreshed data every 10 minutes from NOAA GOES and JMA Himawari-8 satellites, and every 15 minutes via EUMETSAT Meteosat satellites. https://zoom.earth/

10) Analyzing videos

Fake information has been a big problem in recent years. Because it has become difficult to determine whether what we see is true or false. When it comes to video, it's even worse. For an investigator, the basic job is to gather reliable information.

Verifying the authenticity of videos can be difficult. The most common technique used to mislead the public is to take a piece of video and paste it on top of another, completely changing the context.

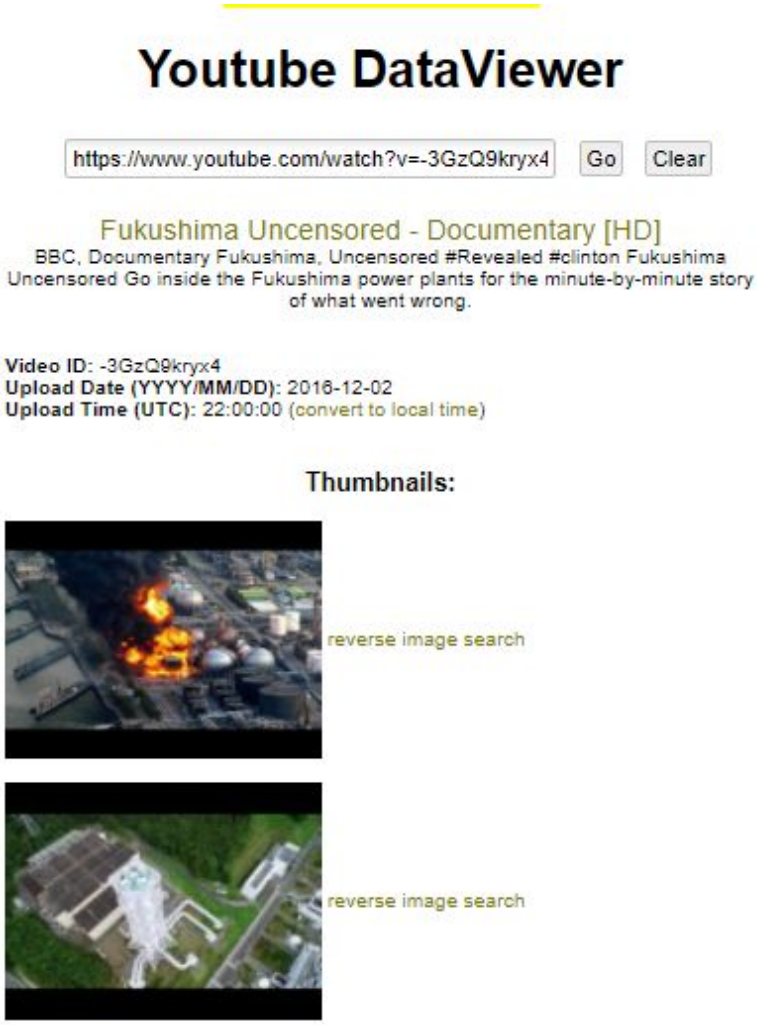
One of the best ways to uncover these kinds of schemes is to compare the images in a video with other images online. This way you can find out if there are any matches that indicate the origin of the video is different from the description that accompanies it.

An excellent tool for detecting fake videos is the **YouTube Data Viewer** developed by Amnesty International. This tool is easy to use: you insert the url of a YouTube video and click on "Go." The first thing the tool will do is search for metadata about the video, such as the date it was uploaded, which is already important information.

But the most useful feature of the You Tube Data Viewer is that it will deliver a series of thumbnails of the video. Once available, you can use these to do a reverse image search which can help you determine if these images appeared in a different version of the video, in a different context or location.

If you go directly to You Tube, you can type in the name of a location where the video is supposed to take place and you will receive links that allow you to compare the different locations.

https://citizenevidence.amnestyusa.org/



You may also need to carefully study a video and **"The Anilyzer"** allows the user to view videos frame by frame and in slow motion and it's a free service.
http://anilyzer.com/

To work on a video from You Tube, it is interesting to be able to download it. There are lots of sites that offer this very useful service for an investigator.
https://www.4kdownload.com/
The same goes for videos from Twitter and Facebook.
https://www.downloadtwittervideo.com/
https://www.downloadvideosfrom.com/
As with a photo, it is sometimes useful for an investigator to have access to the metadata of a video: file size, copyright, file type, keywords, description etc.
https://www.metadata2go.com/

11. Tracking a target by sending them a detection link (Canary Token)

A **Canary Token** is a customizable tracking link, useful for tracking who clicks on a link and where it is shared. Canary tokens come in several types. The idea is to leave tokens on your network so that intruders can warn you when they start doing things they shouldn't.

Basically, it's the principle of the honeypot that you place somewhere you know the target is going to come and poke their nose into, or you send it to them in such a way that it's very tempting to smell the sweet scent. The second option is of course the most tempting.

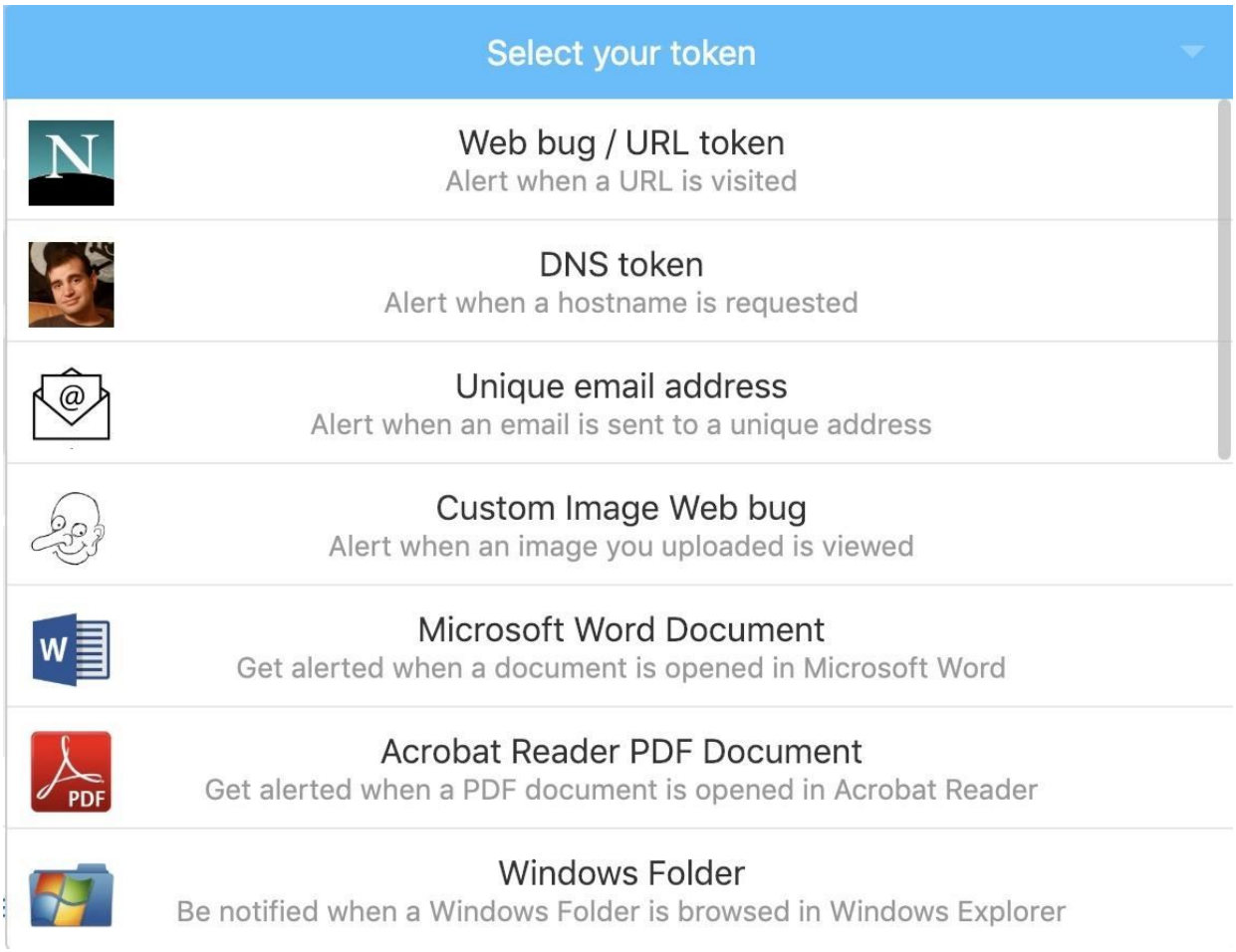
This is exactly what the Canary Token site does. You sign up, and the site generates a unique identifier that you can then place as a link in one of your emails or any other form of contact with your target (Why not via whatsapp?). The honeypot principle is not new but what existed before this site was reserved for people with strange skills using languages unknown to most humans.

Canary tokens are designed to be so simple that anyone can use them. Depending on how you deploy them, they can detect when someone clicks on a link, opens an email, shares a file or otherwise interacts with the tracking link.

This is interesting when you need to locate a person, for example in the context of tracing a debtor or if your company is being harassed by a blackmailer. Canary Token is basically a computer security tool, created to identify a hacker accessing your data but it can be used more offensively. Being careful, in the end, we will find the IP address of the target. If it is an IP used on a corporate network, you have a chance to locate it accurately. If it is a private one, you will find the city at best. If it's protected behind a VPN, you won't find anything at all.

You don't need much to get started: a browser and an email address.

On the Canarytokens website, you can generate a Canary token by clicking on "Select your token" and choosing the type you want to create.

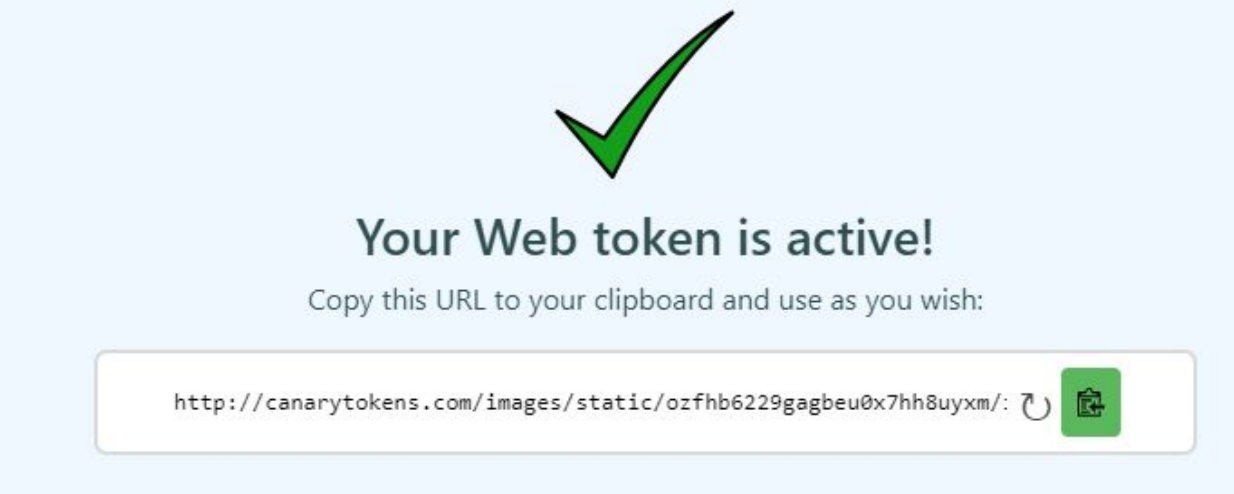


The simplest type of link to generate is a "**Web bug / URL token**" which will trigger an alert whenever someone clicks on or shares the link. This is a link to a website, but there are also several other options.

A **"DNS token"** creates an alert every time a URL is requested, whether the web page is actually loaded or not. Other available Canary tokens are files that report on the opening or browsing, available as Word documents, PDF files, a photo etc.

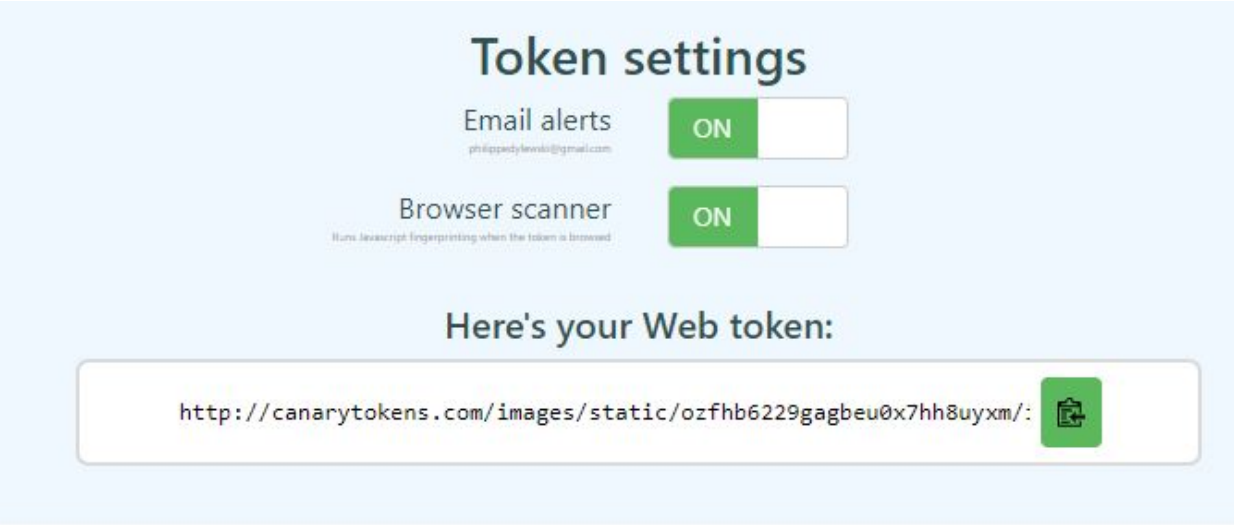
Next, enter the email address from which you wish to receive notifications. You can also skip this step and simply configure it via the web interface, but if you lose the link, you'll have a hard time interacting with the Canary tokens you've created.

Then click on "create my canarytoken".



Click on "manage this token" in the top right corner, and you will be taken to the page that allows you to monitor and control the Canary token.

You should see something like this:



There, you have your trap. Well, not because to actively trap your target, you need to be able to send him/her an email, a skype message or a whatsapp with a content so attractive that the person will want to click on the link.

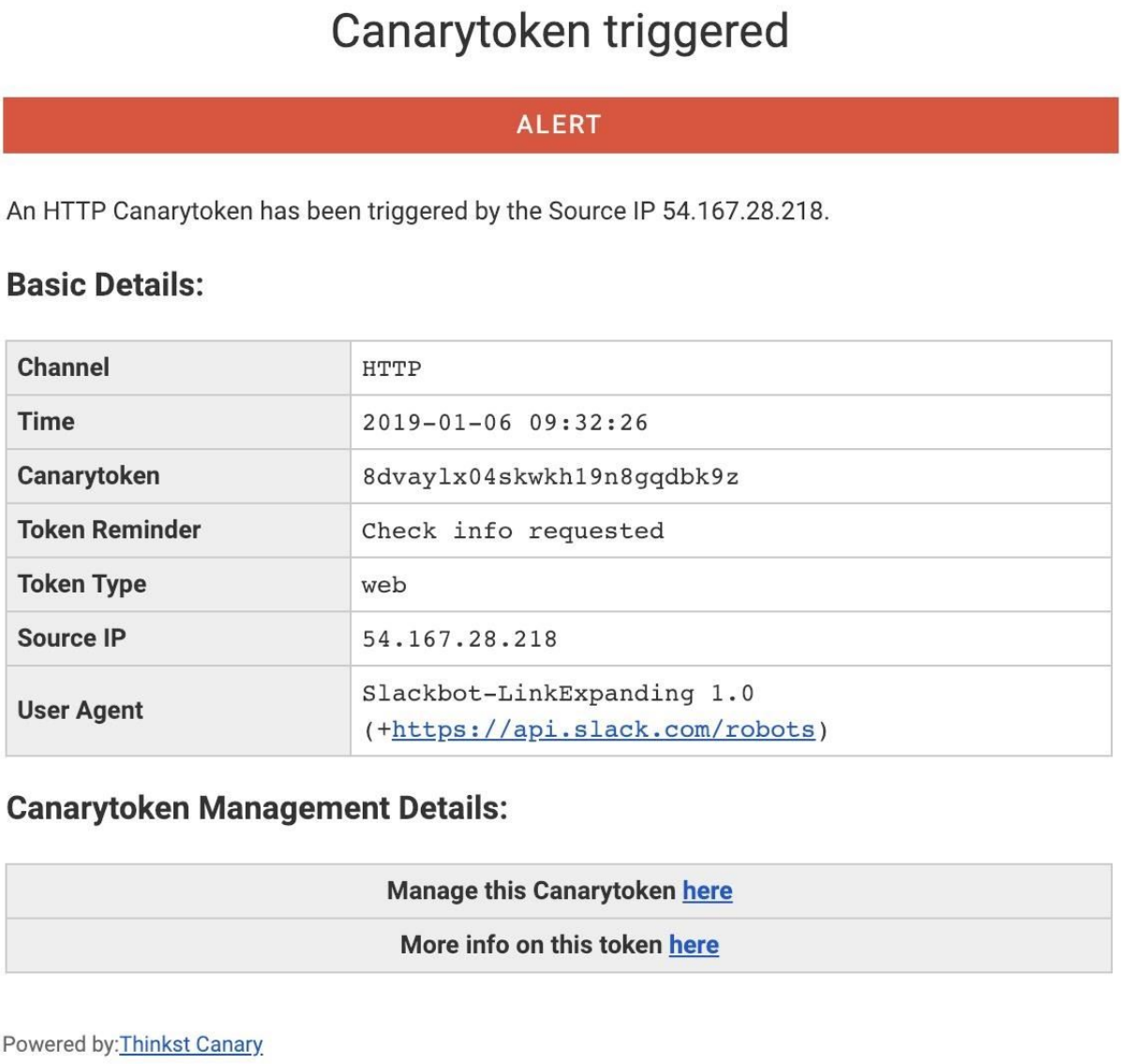
If you do a test by launching the token via your browser, you will just see a blank page, which is normal.

I suggest you use a VPN (see the chapter on VPN) before launching. This will prevent you from getting backlash from your target.

Another way to use a Canary token is to shorten it with a URL shortener. You can use services like **Bit.ly** to hide the actual URL. This allows you to create a smaller, less suspicious token. https://bitly.com/

After adding your Canary token link to Bit.ly, you can use the shortened link in the same way you would use the original. Often, this shortened link will attract less suspicion than the super-long URL of the Canary token.

As soon as your trap works, you get this:



Canarytoken triggered

ALERT

An HTTP Canarytoken has been triggered by the Source IP 54.167.28.218.

Basic Details:

Channel	HTTP
Time	2019-01-06 09:32:26
Canarytoken	8dvaylx04skwkh19n8gqdbk9z
Token Reminder	Check info requested
Token Type	web
Source IP	54.167.28.218
User Agent	Slackbot-LinkExpanding 1.0 (+https://api.slack.com/robots)

Canarytoken Management Details:

Manage this Canarytoken here
More info on this token here

Powered by:Thinkst Canary

The interesting information is in "IP source". All you have to do is enter the address into an IP address locator, which we have seen in an earlier chapter.

And if that didn't work, if your trap didn't close, you can refine your method by using other tokens, with other file types. This will require a little work, a little study, but nothing that requires a degree in computer science. The reason I am suggesting Canarytokens is that it is a tool that is accessible to most people. You can make mistakes, but you will understand. You will find on the site and everywhere on the net, recommendations to use the best performances of this site. But you can start practicing with your friends and family, just to get the hang of it. https://canarytokens.org/

IV. Techniques and tools for sourcing candidates

I created and managed a recruitment agency for 15 years. What I liked most about the job was sourcing candidates. I found the interviews boring most of the time and as soon as I could, I delegated this task to the team. Everyone was happy because it was the boss who was doing the job that nobody wanted to do. Later on, I had a change of heart: my choice to be a "headhunter" had to be taken in a more down-to-earth sense and I sold everything to become a private detective, very active in the search for missing persons. I was finally a real headhunter. This did not prevent me from keeping a foot in recruitment by offering candidate sourcing and CV checking activities (background check).

Whatever the economic situation in a country or region, finding good candidates is never easy. This is because unless you are in a unique business, the candidate you find interesting will also be found interesting by other recruiters. This chapter is aimed at professional recruiters as well as those who recruit on a casual basis. It focuses exclusively on finding candidates through techniques and tools. But if your job is not recruitment related, this chapter may still be of interest to you because the techniques seen here can be combined with other types of assignments.

1. **Finding emails from LinkedIn candidates**

Theoretically, it is no longer possible to export the email addresses of your LinkedIn contacts. It was a nice feature, but it's gone. As our intelligence is largely defined by our ability to adapt, let's see what we can do.

Contactout is an email address scraping tool. In short, Contactout is able to instantly find the personal email address and phone number of potential candidates on LinkedIn by automatically searching other social media sites and the web in general using an artificial intelligence engine. It doesn't fall into the trap of other LinkedIn scraping tools that spend their time trying to bypass the site's security. When they do, it's usually for a few days or weeks. Contactout is an extension for Chrome. So you need to install it on your computer. Contactout promises full verification of the emails offered. The

only thing I fear is that it won't last. Contactout is almost unanimously considered to be the best in its category. https://contactout.com/

AeroLeads is a good tool for generating leads or applications with very good accuracy. It is a versatile tool unlike other tools that can only find emails or simply add leads to CRM databases. On your Aeroleads dashboard, you can find the added candidate with their name, title and employer.

In addition to this, you can find the candidate's email and phone number.

You can test Aeroleads and if you like the tool, it will cost you a minimum of $49 per month for a database of 1,000 prospects/candidates.

This is a Chrome extension that scrapes directly from LinkedIn via your account. It is of no danger to your account, but don't expect hundreds of candidates per day. You will have to respect LinkedIn's security rules. Aeroleads is not the first tool of its kind, far from it. I've used lots of them, both for prospecting and for recruiting. What sets Aerloleads apart from the others is that it's always there, because LinkedIn doesn't like these scrapers at all and most of them disappear after they have proven their effectiveness. https://aeroleads.com/

2. Automating the search on LinkedIn? The limitations of LinkedIn and how to get around them

Searching for and contacting potential candidates on LinkedIn is not a very fun activity. It's hard to put it any other way. I'm talking about active search, the kind where you look for contact. I'm not saying that looking for candidates is a bad method, but sometimes it's not enough. If no one comes to you, then you have to go look for them.

Once I have a list of potential candidates, I send them an invitation without a message. This is much faster and more effective. This method, if you have a halfway decent profile, will get you about 30% acceptance. It is to these people that you send a message. This is because if you make an acceptance request with a message, many people will accept your invitation without paying attention to your message and I find it embarrassing to send the same message twice.

Are you considering automating some of the lead generation processes on LinkedIn? Read this first, otherwise we disclaim any responsibility for what might happen to your karma.

Why can't I connect to a million people in 5 minutes?

For one thing, LinkedIn collects, hosts, protects and organizes our data so that it is the best place for professionals to meet, exchange, learn and work together. They do a great job and are useful to hundreds of millions of people around the world. Good for them! But on the other hand, the data on LinkedIn is YOUR data, OUR data, and LinkedIn would be nothing without it. So charging hundreds or thousands of euros a year for everyone to access their peers' data is a high price to pay when you are giving your data away for free. So it is ok that LinkedIn puts up safeguards. That's fair enough. If LinkedIn became the kibbutz of information, it would be a bit of a mess and probably the end of their business model. I often agree that the rules exist, as long as they don't apply to me, or I can find a way not to comply with them.

First, let's get inside LinkedIn's head: What do they want? Real people, who give them real information, who keep it up to date, and incidentally who become paying users, which is their goal.

The more they get what they want, the more they will reward users with more visibility and access to information.

Here is an (incomplete) list of factors that will impact your own action limits:

- Whether you have a paid subscription. This is a very important criterion, as firing a beggar is not the same as blocking a good, fat customer.
- Date of creation of the profile.
- Richness of the profile.
- Number of connections.
- Time spent per day on LinkedIn.
- Number of messages sent per day.

- Amount of pending invitations. The less the better. Above 1,000, you are suspected of spamming, the ultimate crime.
- How many articles and publications you publish.
- How many comments or ratings you give.

What are the limits before you get slapped on the wrist?

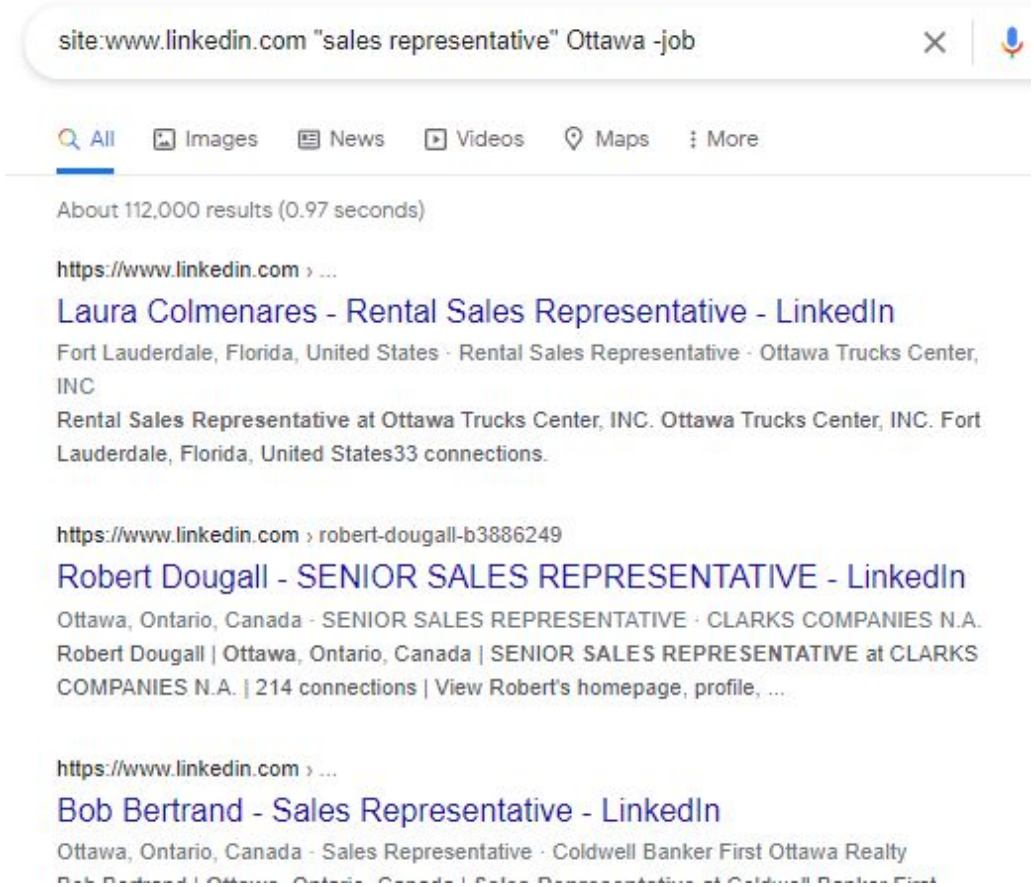
The latest Linkedin update has caused quite a stir among recruiters: even with a Linkedin recruiter account, it is now only possible to send 100 invitations per week compared to 100 per day before.

LinkedIn says that if you exceed the limit, your account can be deleted. This is possible, but the reason they didn't do it with me is that you can push the limits of use. When I was using a free account, I was regularly blocked for several days. This has as much to do with the usage limits as it does with the people I contact. If many of the people you contact say they don't know you, you can be blocked quickly. In recruitment, this is much less likely than in cold calling. As a recruiter, you are much less exposed to this problem than a Commercial. It is rare that a person feels attacked when receiving a job offer, but it can happen when someone is prospecting you.

How to get around the limits of use

If your search is one-off and you are poor, you can take out a premium subscription, with a free trial for one month. If you don't want to pay anything, take the subscription that offers you access to an unlimited number of profiles. Two or three days before the end of your trial, cancel the subscription and your credit card will not be charged. LinkedIn is impeccably honest about this. The method is a bit mean if it is to earn a few pennies. It is much less petty if you want to test a service before paying for it, because the free trial version gives you access to all the features.

Another method, which gives you unlimited and free access to LinkedIn, is the Boolean search via Google, which we have seen in earlier chapters. Since all LinkedIn data is indexed in Google, you can search for as many profiles as you want with no limits.



I made a search for a sales representative in the Ottawa region in Canada. After noticing that I was receiving mostly job offers, I started the search again, indicating in my query that I did not want any job offer ("-job"). While the method is free and very sophisticated, it will require a good level of Boolean search skills. The good news, we saw in an earlier chapter, that there are Boolean search engines exclusively targeting Linkedin.

If you absolutely want to automate certain tasks on LinkedIn, you have a choice. There are hundreds of them. Most of them are extensions for Chrome. For me, they all have the same negative point, but it's personal. The extensions that survive LinkedIn's wrath are the ones that respect the usage limits to the letter. I don't like limits.

If you want to automate your activity on LinkedIn, Dux-Soup is the most efficient way. Using a simple Chrome extension, you can automate the process of sending personalized messages to candidates, following up with automated replies, approving connections and tracking profiles. In addition you can integrate much of this activity with your CRM.

Despite its odd name, Dux Soup was one of the first LinkedIn lead generation tools I used. Unfortunately, like many things in life, Dux Soup should be used in moderation when it comes to leveraging its powerful tools. "Moderation" is not precisely a word I like.

Dux Soup can be downloaded for free. Most of the useful features are paid for and can be purchased through a monthly or annual subscription. This Chrome extension helps you put your candidate generation on autopilot by automating tasks such as posting profiles, sending invitations and messages.

Note that this tool is considered "cheating" in the eyes of LinkedIn. If you misuse this tool and increase the settings too much, you could receive a warning email or even have your account suspended. Using Dux Soup takes some time, especially when, like me, you are not a super fan of technology and want to use the advanced settings of the extension.

How long will Dux Soup last? Dux Soup directly violates LinkedIn's terms of service, and that could mean that it could disappear tomorrow. LinkedIn could try to sue Dux Soup, or more likely, release an algorithm update that breaks or disables features in Dux Soup. The result is a cat-and-mouse game between the two companies, where one breaks a feature and the other fixes it as quickly as possible.

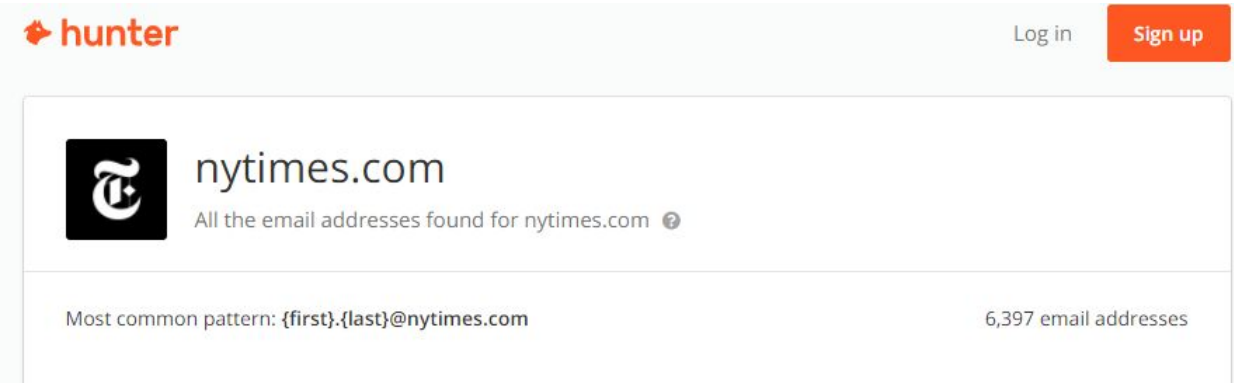
Although this has not yet happened in any significant way, it could happen. So it's important that if you're looking for a rock-solid LinkedIn tool, this is not it. But to be fair, no LinkedIn automation tool will be. That's just the risk we take when we use certain tools to get ahead. Although LinkedIn officially states that automation is against its policy, it realizes that a large part of its user base does it. I think LinkedIn turns a blind eye to most automation, as long as they are not excessive or spammy. If LinkedIn wanted to, I think they could write a program to detect the presence of automation plugins, but they don't.

Prices start at $15. I suggest you never take the annual subscription as you can't be sure the tool will still be functional next week. https://www.dux-soup.com/

A serious competitor to Dux Soup is **Prospectin** , which is French and in roughly the same price zone.
https://www.prospectin.fr/

3. Finding emails of people working in the company you are targeting

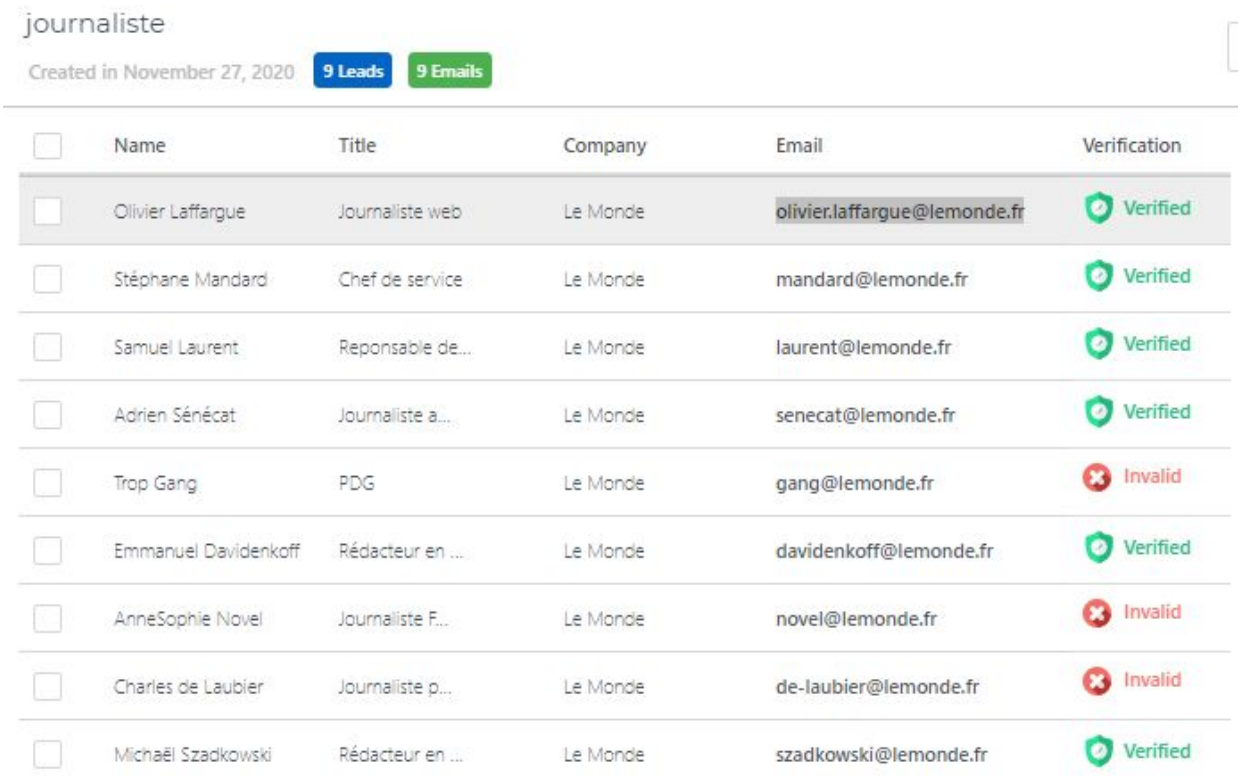
To target a company and get a maximum of email addresses of its employees is possible with **Hunter** . It is easy to use as you just type in the name of a company and you receive in a few seconds the email addresses of people working in that company. For example, to promote this book, I send an email to a maximum number of journalists for example those at The New York Times



Hunter offers me 6.397 email addresses. The question is that: Are they all journalists or are all the addresses active? May be not, but in addition to the list of addresses, Hunter provides me with the links that made it possible to find them. This means that if a link doesn't match my search or I think the links are too old, I can destroy the address and then export the results in csv format. The free version allows me to do 50 searches per month, but I only have access to 10 emails per search. The first price is $49 per month. https://hunter.io/

https://email-format.com does the same job as Hunter. It's free, but not as good because the proposed addresses seem a bit fishy.

Skrapp hunts down email on LinkedIn and brings back information in a very structured way. In addition to a free offer of 150 addresses per month and an address checker. I don't know how they do it, but the result is there. https://skrapp.io/



If you're the information freeloader, you can go around the email hoovers and accumulate free subscriptions.

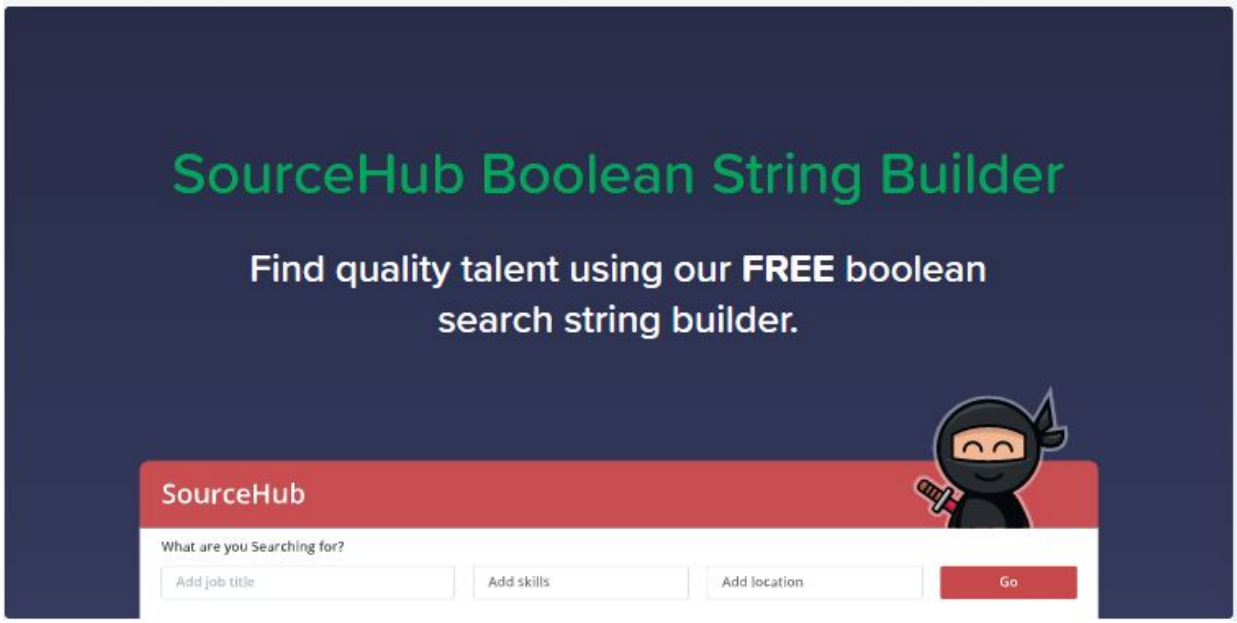
4 – Finding candidates on Linkedin via Google

If you're struggling to master the use of Boolean tools, you'll love **SourceHub** .

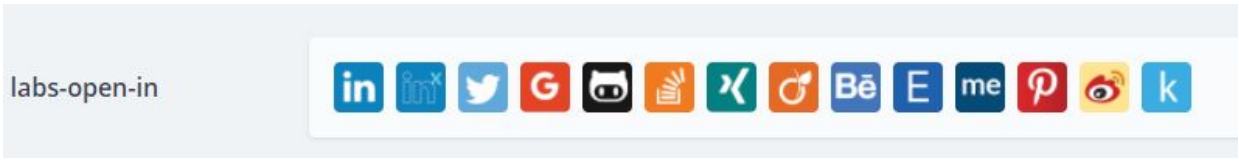
SourceHub takes the hassle out of using Boolean codes, by setting up taxonomies to perform comprehensive searches for you, from very little data. SourceHub allows you to search on LinkedIn, Twitter, Facebook etc up to 15 networks in total. All you have to do is enter the job title you are intending to take on, the skills the candidate should have and where you can find them.

Use No AND, OR or NOT. Just tell SourceHub exactly what you are looking for, in simple terms, and it will do the work for you. You can also exclude terms from your search.

Fill in the fields with the criteria/locations of the candidates.



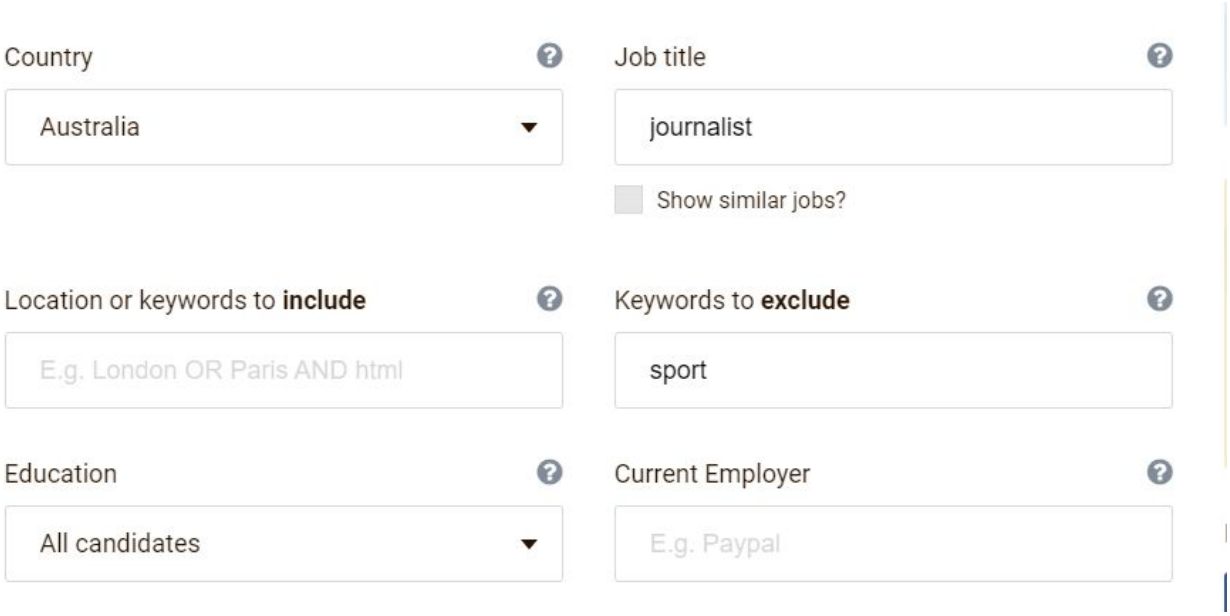
The small challenge is that you need to know that to start the search, you need to go to the bottom of the page and click on the network you are interested in. Special mention for the web search because it allows you to find the profiles of candidates who have created a mini-site to present their application, and there are more and more of them.



https://source.socialtalent.com/

Recruitem is a free tool that allows you to hunt on Linkedin without going through Linkedin. The engine uses Boolean search with a series of criteria of your choice and offers you a series of profiles found on Linkedin.

In the example below I am searching for journalists in Australia , excluding those working in the field of sports. It is simple and perfect.
https://recruitin.net/



Recruitmentgeek does the same job and it's also free though the search engine is less accurate, but that's really to be picky because both tools are great and free!
https://recruitmentgeek.com/

5) Searching for candidates on Linkedin with a free account

I'm assuming that you know about Linkedin, have an account and have some knowledge of the site.

You know that there is a search bar and that when you launch a search, "sales manager" for example, you will get an impressive, and therefore unusable, collection of results.

I also assume that you know that the first sorting of results, once your future sales manager search has come back with thousands of results, is done with the bar above the screen. You can do a first sort if you are looking for people who are or have been sales managers, job offers for sales managers, content where you can read articles related to the terms you are looking for, sales management groups etc.

That's the basic of the basics. I'm not explaining. If you are totally new to Linkedin stuff , you will understand the short paragraph above by trying it out for yourself in 15 minutes. As we are in the context of a sourcing assignment, it is of course the 'people' button that you click on. Having thousands of results is about as hopeless as having none.

You can start narrowing down the search with basic criteria such as geographical location, names of current and past companies, industry sector, school your candidate would be welcomed if graduated from etc. LinkedIn also offers you a choice of the level of relationship you have with the people you are likely to contact. In the context of candidate sourcing, whether the people are first level (already in your relationships) or in the relationships of your relationships, is rather irrelevant.

LinkedIn and the Boolean search

LinkedIn's engine works like Google's. A previous chapter is dedicated to Boolean searches. What I'm going to do here is to give some examples of its application.

I am searching for a medical representative for the Johannesburg region. My client wants to meet candidates who have proven experience in a similar job.

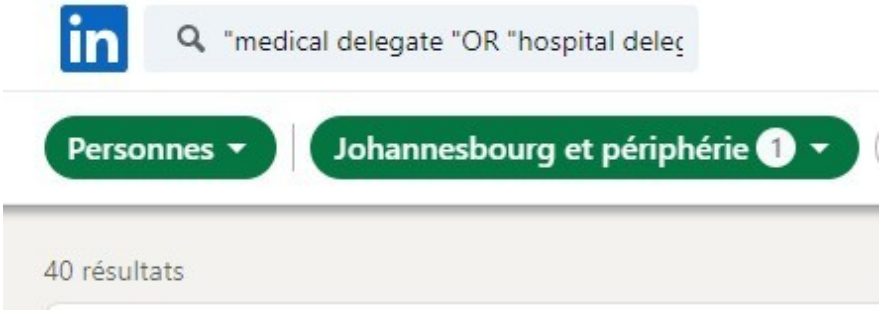
The first level of sorting in Boolean search will be the use of inverted commas. For example, if I search for medical delegate, I get 4.100 results. Because LinkedIn returns medical delegates, delegates of all stripes and anyone with the word 'medical' in their profile. That's a lot of people. And again, I'm not simulating a search where there are terms

This would multiply the results astronomically. Except, of course, that you have already taken care to limit your searches to a specific geographical area.

I end up with 495 profiles.

Above all, my client wants candidates with experience of medical delegation, but only those who are used to visiting doctors or hospitals. He doesn't want those who visit pharmacies because that's a different profile.

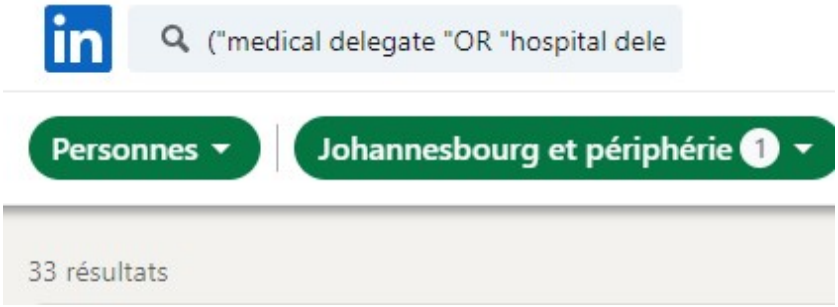
"medical delegate "OR "hospital delegate "NOT "pharmacy" NOT "pharmaceutical"



Here, with the term "NOT", I exclude those who have the word "pharmacy" in their profile and I am left with 40 links. For complex searches, which combine a series of criteria, it would be better to use brackets, which help to structure the search.

("medical delegate "OR "hospital delegate")NOT("pharmacy "OR "pharmaceutical")

Here, I exclude applications that contain either the word "pharmacy" or the word "pharmaceutical".



This leaves me with 33 profiles.

As you can see, the level of technical knowledge to use the Boolean search on LinkedIn is rather low. What makes it complex to use is the ability to structure your thinking and research into signs. With a little bit of practice you will be a prince of tracking.

V. The spy equipment

Like you, I grew up watching spy films. I was fascinated by the charisma, courage and charm of these heroes and also by the power of the equipment they used. The irony of the story is that the equipment used by these agents until the end of the 20th century can be found on sale on Amazon for a few Euros.

I started my career as a private investigator in 2004. To give an example, a GPS tracker was the size of a shoebox and cost a fortune. Of course, there are still services reserved for state services. The average person does not normally have access to them. We can't locate a computer with a single click, and a simple photo taken in the street won't tell us where the person lives or what they had for breakfast. Films are always one step ahead of us. That lead is getting shorter and shorter.

The use of all the tools revealed here is totally illegal when it comes to obtaining information about a person or an organization without their knowledge. You already know this. All the techniques presented in this book have an industrial or commercial purpose and most of those who will use the material presented here will do so to spy on spouses and children. If I were in judgment, I would write about other things.

I have only presented one or two products per category here. Sometimes none, and then a list of the criteria for buying, otherwise this book would be the size of an encyclopaedia. This is to offer preferably the best, or at least the best size of a book for a reasonable price. Material costing more than a few hundred dollars is not presented here. I have also explained the strong and weak points of the product. At the end of the chapter you will find some links to sites where you can buy the material. Finally, I insist on the scams, which are rather rare with the equipment, and on the limits of use, which are often not given by the manufacturer.

1. Spying on a phone remotely

The total intelligence officer's dream is taking control of a mobile phone remotely. First question: is this really possible or is it a scam coupled with a

legend? It is possible but with conditions such that its use in practice is very limited. A costly technique is explained in paragraph 19.

The first constraint is that you must have physical access to the phone and know the opening code and it takes about ten minutes to install the software. Anyone who promises you remote access is lying, even those who say you can do it via a Bluetooth connection, as it will probably be detected by the target phone.

Before you buy, check that your future software is Mac or Pc, Android or iOS compatible, depending on your hardware.

The basic features are keylogger, remote screen capture, access to photos and videos, access to all messaging and social networking accounts of the target and of course, real-time geolocation. These are the legal functions in Europe.

In Europe, it is forbidden to use software that controls microphones, cameras and email software but buying it is easy.

Flexispy is one of the most advanced spy phone applications in the world. It allows you to track SMS, Facebook, WhatsApp, Twitter and locate devices. It is compatible with Android, iOS, PC and iPad.

It is available in lite, premium and extreme versions. All have different features. Once installed, it tracks the call logs and other activities of the targeted phone. To view the activity report, all you need to do is log in to the Flexispy account.

The tool is not cheap. But it is the best and it is still affordable. Budget between 29,95 and 199 dollars per month. https://www.flexispy.com/fr/

2. The spy pen

As the name suggests, this is a genuine pen with the task of filming and/or recording a situation.

In order to earn this title, the pen must:

- Write, I know this seems obvious, but apparently not for all manufacturers.

- Record Sound or film at an acceptable level of quality. Forget about top quality.
- Look like a real pen and therefore undetectable to the eye.
- Have sufficient battery life and a good recharging capacity.

The SIRGAWAIN spy camera pen does all this very well for a budget of 50 euros.

The tool is very good, but that doesn't mean it's perfect. You need to film close to your target and in a bright environment. You need a memory card, which is not included. There is also no image stabilisation tool, so if you are filming in motion, the result will be poor. Finally, the camera does not record sound, but this is standard on this type of product.

3. The drone with camera

There's no need to explain what a drone is, it's something that looks like a toy for kids, with the design of a spider without hair that allows you to fly over a target in static flight.

Of course, watching a target from a helicopter is a different matter when it comes to adrenaline, but when you know that a drone can be bought for 20 euros or more, it deserves some thought.

If you want to buy a drone for your intelligence activities, it is essential to pay attention to a few things:

- The first thing is that the drone is equipped with a camera.
- Controllable from a respectable distance. If you want to observe your competitor's goods movements, it would be a pity to have to do it from his car park. The other reason this is crucial is that if your drone has a short range, you will need to fly it at an altitude where it will be immediately detected. Let's be clear, a drone is not a satellite and is rather difficult to make unobtrusive unless you decide to invest in machines costing hundreds of thousands of euros but which have no place here.
- Image quality and image stabilisation.
- Autonomy.
- Speed can be a criterion, but in intelligence missions, I don't see much use for it.

Here, because of the wide range of prices, I will describe two products. Though I have not used either of them, I have only attended corporate facility security missions.

Snaptain SP 500 . Budget around 150 euros. Battery life is 15 minutes but the drone comes with two batteries. The range is 220 metres. That's good, but it's not the CIA's equipment. It's more of a beginner's tool because its main drawback is that it will be detected by people on the ground. At that price, it's still a very nice tool for detecting problems on your own installations.

The DJI Mavic Air 2 has a battery life of over 30 minutes, takes high quality photos and videos and has a range of 10 kilometres. It has a stabilization feature in the air. It flies at more than 60 km/hour but I don't really see the point of it for the intelligence world. The price is 1000 dollars.

4. The GPS beacon for remote surveillance

The GPS beacon , also known as a **tracker** , is a tool for remote tracking. Beware that it is forbidden to use it without a person's knowledge, and that is why all the sites that sell this type of tool give recommendations for legal use that no one is interested in , but the honor is safe. Anyway, the manufacturer says it's for the safety of your stage 3 Alzheimer's mum or to make sure your teenager doesn't get involved with nasty little hoodlums.

In our world, we use beacons to track a vehicle in real time without being detected. I've done a lot of tailing in my career, in fact it's one of the reasons I chose this job, and I was quickly disillusioned. It's not at all like on TV. In the real world, you often lose your target in traffic, get speeding tickets that your client refuses to pay and its crazy stressful. The GPS tag puts an end to all that with one minor drawback: it's illegal to stick one on your target's car.

The same goes for your wife's handbag, which is now possible because the tracker is the size of a credit card, but thicker.

The other advantage of the product is that it doesn't cost much to track. Before, you needed a whole team of people available 24 hours a day, which the customer found outrageously expensive. Now you are comfortable, you never lose your target and you don't have to risk getting hit by a 30-ton truck because you are obsessed with your target's tail lights. It is well known that most people buy this product to tail their half.

Another great use in industrial and commercial settings is for tracking goods if your business is being robbed, which happens often. With a beacon, if your shipment doesn't arrive where it's supposed to, or disappears from your warehouse, you'll know right away and only have to call the police. Here, the use of GPS is legal.

There are models that can be slipped into a bag or glove compartment, others are magnetic, equipped with magnets, and can be placed on a metal support. The latter can be attached to the underside of a car, as the magnets are strong enough to withstand the shocks of a country road.

The GPS tracker can have several uses. It is safe to protect or find, and it can obviously be used to track someone. It works by GPS combined with communication to a smartphone,

You can use it to find out if your salesperson is spending his or her days at the customer's premises rather than in the pub, but you won't be able to use this information in court.

The criteria for choosing the GPS you need are

- Size
- The autonomy. This is a difficult choice because if you want a long battery life, you will need a larger battery, which will make the tracker larger and therefore less discreet. It all depends on the use. A plotter in a container doesn't need to be especially discreet.
- Ease of installation and attachment. The provision of a magnet is essential if it is to be fitted to a vehicle, if you cannot access the interior of the vehicle.
- Supplied with a waterproof case
- Operating costs
- Choice of SIM card

- Choice of operator

When purchasing a GPS tracker, subscriptions or packages with an operator are not mandatory. There is nothing to prevent you from deleting the PIN code from the SIM card and activating the SMS function to make the GPS tracker operational but with a subscription, you will be able to track the target in real time, whereas otherwise you will be informed regularly by SMS of its position. If it's for tracking, the question doesn't really arise because you need to know where the target is at all times, but if it's for tracking goods, I think it's much less essential. Finally, remember that technology has progressed dramatically in the last 20 years. Talking about a GPS tracker doesn't even make sense anymore because the question is: what tracker do I need?

Look at this little gadget, **the Cube** . It's tiny, it fits in a pocket or a bag. It costs about 20 euros, so losing it is not a big deal. It does the job, but if you want to track a container for 2 months, I don't think it will be the ideal tool.

5. Look under the door. The endoscope

The **endoscopic camera** is traditionally used in medicine and industry. Its job is to see where it is difficult to see with the naked eye, whether it is your butt or the inaccessible part of a facility.

We've all seen it used in movies or news reports by elite police teams to prepare for an intervention when it comes to seeing what's going on the other side of the door, behind a window or below the ceiling. So clearly this tool can be a valuable ally to the intelligence officer.

Image Credits: Amazon

The criteria for choosing an endoscope are:

- That it is battery operated and not mains operated. It's not a good idea to have to look for a plug in the middle of the night.
- The battery life. This ranges from 30 minutes for entry-level scopes to several hours.
- The length of the cable.
- The quality of the cable.
- Waterproof camera.
- Image quality. Full HD is a minimum.
- WI-FI function with mobile application.
- Brightness adjustment.
- Zooming.
- For the higher end, does not require the use of your smartphone but works with a stand-alone box that offers more functionality.

- Comes with additional tools such as a pole if the camera needs to be placed high up, a clamp to pick up small objects or a mirror to see at 90 degrees.

The above criteria are not necessarily quality criteria. As is often the case with equipment, it is a matter of buying what you need. If you have to run the cable under a window and you are hiding behind it, you don't need a long cable.

The budget for entry-level stuff that works properly is 30 to 35 dollars. Don't think that these very low prices are an indication of poor quality equipment. You get what you pay for. The top of the line industria l tool will cost you between 180 and 300 dollars.

6. Listen through the door or wall. The stethoscope

Wall contact microphones are professional devices, used for investigative, private or military purposes. These devices will help you to listen to conversations through walls in a confidential and safe way, without the risk of being detected. Let's take a look at what wall microphones are used for and what their components are, in order to fully understand all the features of these listening devices.

A wall microphone is used to hear through walls, all types of sounds, thanks to sensors in direct contact with walls or ceilings up to 70cm thick. A contact microphone consists of a microphone capsule, a diaphragm that transforms sound vibrations into audio signals, a voice processor and a preamplifier. An earphone or digital voice recorder can be connected to the audio output. These tools are able to detect even the faintest of noises, resulting in clear and stable sound. These investigative devices are very good value for money. This is obviously much better than the good old doctor's stethoscope. Don't buy one for your intelligence missions as it won't pick up all the sounds.

Please note that the key words to find these products are NOT "stethoscope", but rather "wall microphone", "spy stethoscope", "wall listening"etc.

Prices for this material range from 15 to 200 dollars. Some products have a high penetration power, but in general you don't need to cross more than 25

centimeters. Also check that it is possible to connect your device to a recorder, at least if you need to keep a record of the conversation being spied on. Finally, some devices allow you to sort out the different sound levels. In practice, entry-level equipment is quite good here.

7. Seeing without being seen: the mini spy camera

A good spy camera can have all sorts of uses, even for those of you who are not secret agents. Good spy cameras come in many shapes and sizes and can be used for home security, as well as to monitor children and pets when you are not in the room, or to illegally film your employees wringing out your stocks to ensure a fat end of the month. Again, any illegally obtained information will be of no use to you in a court of law as you will not be able to present the evidence obtained, even if it is factually incontrovertible.

Cameras are generally inexpensive, and some are even disguised as household items such as clocks or glasses, allowing you to be very discreet. Some are simple little cameras the size of a two-euro coin, and sometimes even smaller, that can be placed in a place where most people won't notice them, while others are disguised as objects such as photo frames or USB sticks. As you can imagine, there are many creative possibilities in this area.

Spy cameras usually have a wide-angle lens, which allows them to capture as much space as possible in a given area. Video quality tends to vary. Some provide basic, functional video, sufficient for you to see what is going on in the area is happening, while others produce high quality images.

Some spy cameras also offer useful extra features such as night vision or motion detection, which means they can stay on longer without needing to recharge their batteries.

Another advantage of the mini camera is its ease of use. You don't have to be an expert to set it up. I am not well versed with technology. However, it didn't take me 15 minutes to learn how to install this kind of equipment.

What are the purchasing criteria? Of course, these criteria are more or less important depending on the use you expect of the camera.

- The autonomy. This is the weak point of this equipment. An autonomy of one hour is already a good result for a live recording. If the camera records on a memory card, you can have a battery life of two to three hours. Some cameras can be plugged into the mains, but for discretion, this complicates matters.
- Supplied with various brackets. For example with a clamp.
- The solidity of the material and the resistance to shocks.
- Video quality. Full HD will be the minimum definition.
- Equipped with a motion detector that saves battery power since it only triggers if something moves in the environment.
- Night vision mode.
- Sound recording and audio quality.
- Magnetic back so it can be quickly placed on any metal surface.
- Live view or recording on a memory card. To see what is happening live, a WI-FI module is required.
- Waterproof case for outdoor and underwater recording.
- The angle of view.

Prices for a spy camera start at less than 20 dollars. At that price, don't expect to play James Bond. Depending on what you need as options, expect to pay between 30 and 100 dollars.

Some more exotic models of spy cameras

Spy glasses with built-in camera.

Spy glasses are perfect for voyeurs who want to keep a souvenir of the beach and ideal for tailing. On the one hand, you can film hands-free, and on the other hand, if you want to keep a record of your surveillance, you can be on the move while filming. It sounds like an unnecessary gadget, but it's not. There are city models and sunglasses. It is a good tool when you need to film while on the move or for any place where cameras are not welcome.

Before buying, check that the camera is not visible. On the lower end of the market, it's borderline pathetic and ridiculous. Don't expect to produce a quality film. The image is often a bit weak and most models are very sensitive to light. As soon as it gets a little dark, you can't see much. The purchase criteria are more or less the same as for a mini spy camera. Be aware that some models allow you to take pictures and others do not. Do not buy anything under 60 dollars if it is for professional use.

The light bulb camera is a real light bulb, which emits real light and is installed in a room where you want to film and record. It looks great for

filming a meeting, for example. But it's better if the lamp is on when people enter the meeting room, because the camera is still visible. We rely on the fact that we don't like to look at a light source.

There are lots of mini spy cameras. Make your choice according to your needs:

- Wall clock
- Alarm clock (for those who still use one)
- USB stick
- Screw

- Bottle (this is a real plastic bottle)
- Socket
- Watch
- Cap
- I saw one hidden in a deodorant and another in an electric toothbrush.

8. Discreet observation in an urban environment: the monocular

Monoculars are like binoculars for one-eyed people. When you are observing in the city, binoculars lack discretion. Some spotting scopes can be held in one hand and are very handy for identifying a number plate, for example.

There is a wide variety of models and sizes, depending on your use. You have night vision scopes, tripod scopes for long distance observation and even replica pirate scopes. For this last model, I have never tried one and I don't know if aesthetics has replaced efficiency.

Prices vary from 20 to several thousand euros. If it's just for discreet observation in town, the entry-level model is what you need.

9. Jamming the signal of a mobile phone/WIFI network or GPS signal

A simple phone can be used to spy on a sensitive meeting. It is even an excellent way to do this because, unlike the equipment shown here, if the phone is seized, the owner will always be able to say that he just forgot his phone. The best spy equipment is that which is used for its intended purpose and not for its original purpose.

A scrambler ensures that no sound will come out of the room you are in. It would be very useful for teachers who lose their minds when their students are playing with their phones throughout class. The use of mobile phone jammers neutralizes this threat. No more Facebook during a class on the history of the French Revolution. When a jammer is activated, all mobile phones in the jamming coverage area are blocked. Great corporate comedians have also used it to cut off the communications of their unloved boss. The investment is a bit high for a good fat joke, but as I've seen it done, I'll quote it. I agree that seeing your boss shake his phone to get it to

work is one of life's little pleasures. It can also be fun on the train or metro when your neighbor is screaming into his phone.

Finally, and most embarrassingly, unless you are a burglar or an unwanted visitor, many home alarms are wireless systems. The attempted burglary by jamming prevents the transmission networks from working.

Communication between your alarm system and the monitoring Centre is via the GSM network. If the network is blocked, the location is simply no longer protected.

A jammer has a dual purpose: to protect you or to cover your operations.

I have not found any European companies selling these products, but sites in approximate French or English with obviously bogus comments. This doesn't mean they are scams but probably mirror sites that source from Alibaba. Everything I see is from China. I received one as a gift a few years ago and didn't ask where it came from. Though I know receiving a gift like that is weird. The world of private intelligence is weird.

Your scrambler will probably take more than a month to arrive. This makes sense when you consider that such equipment is banned in Europe. So it will be either from Alibaba or EBay. The cost is from 100 euros for a scrambler effective at a few meters. Several hundred euros for beautiful equipment that interrupts mobile telephony, the wifi network and GPS signal. You can easily buy one, but there is always a small risk that it will be seized at customs.

Before buying, check that the frequencies used in your country match the frequencies compatible with the jamming device.

10. Detecting microphones in my office

The problem with microphone detectors is that if your device doesn't find one, you may not know if it's because there are no microphones hidden or if it's because your equipment is worthless, or that you don't know how to use it. I think I've used this equipment three times in my life, and honestly I felt a bit out of place. One day I was at an important client's office and he was convinced that there were bugs hidden in his office because confidential information had leaked. I told him that this was not my specialty, but as we

got on well, he insisted that I take care of it. I searched through his office and found nothing. Then a miracle happens as we leave his office. As he closes the door, something, I didn't know what it was, fell on the floor. This gave me an idea. I asked a lady passing in the corridor to go into the boss's office and count out loud from one to ten. I closed the door and we could clearly hear the lady counting. I looked at the client and he laughed. We had found the 'microphone'.

You can easily buy this equipment, but I don't recommend it. If you are worried about microphones in your facilities, get professional help.

11. The sound amplifier

The purpose of a sound amplifier is to listen to a conversation from a distance, in a public space, and with maximum discretion. For this reason, the traditional amplification model has some concerns about discretion. The satellite dish model is very good, but how can you use this on the terrace of a café?

You can find them in toy shops or on nature walks. If your listening takes place in an open environment and discretion is not a problem for you, this cheap equipment will be quite effective.

The best sound amplifiers are those created for medical use. The price ranges from a 25 dollars toy to a 450 dollars sophisticated system. You have good equipment at around 100 dollars.

The device is not invisible, but it is hardly noticeable and, above all, it gives the impression of being a hearing aid, which it is. The right tools can direct the sound pick-up, and eliminate unwanted noise. Some have a dual application, listening in public space and through a partition, but that is not the same use. If you can afford, buy two separate devices.

12. Keystroke recorder

The **keystroke recorder** , also known as a **keylogger** , is a small piece of software that can be installed very quickly on your PC. It records in a dedicated file all the exchanges written on the machine: texts in Word, conversations on social networks, secret codes as well as visited sites.

They are almost always proposed to watch over the safety of our dear children but this is rarely their real purpose. I have done very few spousal surveillance assignments in my investigative career. I hate it and it always ends badly because the worst is often true. One day I took on such an assignment. The guy looked so distraught that I agreed to assist him. The tailing of his wife lasted less than 30 seconds before I was detected. This was either because I was not at my best or the wife was particularly suspicious. As it was no longer feasible to repeat a sting, I suggested that the client install a keylogger on the family computer. When I saw him again a few days later, he confirmed, crying, that the keylogger was working fine.

His wife did not have a lover, but a whole collection of lovers. That was the last time I took on this kind of job.

To install it, you need physical access to the computer. Some keyloggers require access to the computer to retrieve the information, others send it to an address of your choice. Some are undetectable by anti-virus software, others will require that anti-virus software be disabled for your new spyware. The data is recorded in a hidden report, stored on the hard disk. A keyboard shortcut can be used to make the program invisible to the people using the PC. This is clearly for family use and there is no need to use high-end hardware.

"Revealer keylogger is a free tool that does the job very well. However, it has one drawback: although its activity is not visible from the desktop, it remains active in the task manager. Normally, no one ever goes there unless they know about it or have a good reason to check what's running on the machine. But still, the tool is not totally invisible. Test it on yourself first and make up your minds. If it doesn't suit you, you can easily find another one. https://revealer-keylogger.fr.softonic.com/

13. The spy microphone

The easiest option for recording a conversation is of course your smartphone. If you can place it on a desk, everything is fine. But if things get complicated and you have to hide it, the recording will not be there. Especially if you leave it in your pocket during recording as the sound will be distorted by the simple movement of your clothes.

We saw in this chapter that there are spy pens with excellent recording capabilities. I like the idea, but these are not the days of pens and pencils.

There is a whole range of spy microphones available for every occasion to spy on your fellow man. This will be exclusively for information purposes as you cannot use the information obtained in a court of law. The use of the microphone is very broad. The equipment available today is of excellent quality and at more than democratic prices.

There are two types of spy microphones: those that you carry with you when recording a conversation and those that you hide in a place where you will not be during the recording. If you are in the second case, the best

equipment is one that has a SIM card and works with telephone network coverage. You call your spy's SIM card from your phone and hear everything that happens in the room, while recording the conversation. Some models are triggered by the slightest noise. The device is usually only a few centimetres long and is fairly easy to hide. The only downside for me is that if someone finds it, they will have no idea what it is.

14. VPN

A **Virtual Private Network** (VPN) allows you to ensure your privacy and anonymity online by creating a private network from a public Internet connection. It is therefore not offensive material like most of those in this book. Exceptionally, we will play defense.

VPNs hide your IP address, so that your online actions are virtually untraceable. Surfing the web or transacting on an unsecured Wi-Fi network means you could expose your private information and browsing habits.

Another advantage is that if you want to access the services of a foreign site, you will find that sometimes you will be denied a connection because you are in a country where the service is not accessible. With a well-configured VPN, you will be able to make any site believe that you are in any country. For example, living in Thailand, without a VPN I can't access some Belgian or French online TV channels, which is not the end of the world, but imagine you live in a country where Facebook or Google are banned.

If you bought this book, it may be out of curiosity but it may also be because you intend to use it to do intelligence work. In case you are just surfing the net to glean information, you don't really need a VPN but if you start conducting more aggressive operations and don't want to be detected, a VPN is essential to hide your real IP.

If you are doing some shady stuff, and again it all depends on how much, it would also be good to have a dedicated computer for your mission and why not, use the WI-FI of the MacDonald's in the next town? That being said, if you do some really bad things, even the MacDonald's WI-FI won't protect you because there are surveillance cameras.

Your phone can tell you if there is an open WI-FI nearby but it won't tell you if there's one a hundred yards away. Swedish company Instabridge thought it might be useful to know this without having to spend time walking around the streets with your nose glued to your screen. The WI-Fi doesn't have to be free, as Instabridge not only tells you where the next spot is, but also offers you its password.

App to download at https://instabridge.com/en/

Some criteria for choosing your VPN:

- **Simplicity** . A VPN in English will often be easier to use but in general, using a VPN does not require you to be an engineer. If I can, anyone can. It's just a matter of downloading a software and configuring it a bit. As I'm not here to discuss your connection to Netflix US or an illegal download site, but in your upcoming intelligence missions, basically all you need is to not be traceable and believed to be in a country you are not. Even if you have the IQ of an asparagus, you should be able to do this in three clicks.
- **What you want to do with the VPN** ? Are you targeting a particular country, need access to many countries? Some VPNs don't give access to all countries.
- **Compatibility with your machine .**

There are many free VPNs, but I do not recommend them. They are generally less secure and less efficient.

Practically all VPNs are equal and paid subscriptions are very cheap. For my part, I have been using Cyberghost for a long time. It's one of the world leaders if that's any consolation. https://www.cyberghostvpn.com

15. Hard drive or phone cloning

Forensic cloning , also known as **forensic image** or **bitstream image** , is an exact, bit-for-bit copy of a piece of digital evidence. It captures everything from start to finish. Using this method, files, folders, hard drives, etc. can be cloned and preserved completely and identically.

Forensic mobile phone cloning involves producing an exact copy of an entire mobile phone record. It is carried out on mobile devices that could be

used as evidence in court.

Cloning is not the same as copy and paste. You'd think it would be, but it's not. Forensic cloning is an exact copy of digital evidence, including all deleted or destroyed data, whereas copy/paste is only about the files and folders on the device.

Data found through forensic cloning can be used as evidence in court. Unless you obtained the information illegally.

There is a lot of software available for scanning a PC or a phone. If you need to have a perfect scan of a device, if you need to recover deleted data or if the device is partially destroyed. If you are not a computer forensics speciali st, don't even think about it, or rather, do, but call in a professional.

16. Cryptographic tool

Cryptography is associated with the process of converting ordinary text into unintelligible text and vice versa. It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it.

An example of basic cryptography is an encrypted message in which letters are replaced by other characters. To decode the encrypted content, a grid or table is needed that defines how the letters are transposed. This method has been used for centuries.

Today, there are cryptographic tools and these tools of course use computers. You use them to ensure that your sent emails are only understood by the right person. To make it impossible to read the documents you write or to prevent access to your data if you've done something really stupid and the nice policemen seize your computer equipment before sending you to a cell to relax.

The days of sending encrypted messages using only moving the letters of the alphabet are a thing of the past and a bit out of date.

Writing a message where P becomes W is an example. The code is very simple to break.

Axcrypt will do the job very well, without having to pay for it, if you are on Windows. If you have a Mac, we assume you can afford it and you will have to pay. An IOS or Android version exists for your phone.

https://www.axcrypt.net/

17. An anonymous disposable phone

For some years now, it has theoretically not been possible to buy a disposable phone with an integrated SIM card anonymously. In their legitimate fight against thieves and terrorists of all kinds, many governments have required that the purchase of a SIM card be linked to identification. This is very moderately convenient for someone in the intelligence business.

An anonymous phone has two essential functions: to make or receive anonymous calls and to be as undetectable as possible.

In a perfect world, the disposable phone is ready to use: battery charged, SIM card built-in, with credit. You can find this in any shop, but it won't be anonymous.

You will have to buy both separately.

Your phone will have the following essential features:

- Not a smartphone. A smartphone helps you track yourself with the online applications you use. So look for an old-fashioned phone without internet. Nokia made the best, most solid, and with a battery life of up to a week.
- That it will never be used to call a loved one.
- That it will never be opened in a place you regularly visit.
- That it will never be turned on next to its big brother, your smartphone.
- That it will be switched off when you are not using it and packed in a "silent pocket" that prevents the emission or reception of waves. You can find them on Amazon without any problem. You don't need to be anonymous to buy one.

But you still need a SIM card and a top-up. You can find them in countries like Thailand or Ukraine. You don't need to go there, you can have it sent to

you by post. Remember to buy heavy top-ups because the calls will cost you a fortune. Alternatively, there is a site where you can buy anonymous SIM cards: https://simslife.fr/

The site does not seem to be located on European soil. I can't locate it. I don't blame them for not wanting to be traceable. If you use this SIM card with a smartphone, remember that it is exactly the same as if you were calling from abroad. Disable some functions on your phone, otherwise your credit will be eaten up in ten minutes.

18. A SIM card reader to read SMS from a switched-off phone

If you want to read the SMS messages sent by your target, this is possible without having to install spyware. To do this, you need to get the SIM card from the target phone, insert it into the card reader and connect the reader to your PC. You will have access to the SMS messages on the card, including those that have been deleted. The SIM card reader will not allow you to access the target phone's messaging applications or social networks, but is still a good source of information when you can access the target phone for a few minutes but do not know the access code.

19. Listening in on a remote mobile phone. The IMSI Catcher

You've seen those agents in a movie who connect with two clicks to their target's GSM network to quietly listen in on the conversation. If you had a toy like that, what would you do with it?

An **IMSI Catcher** is an intrusive technology that can be used to locate and track all mobile phones that are switched on in a certain area. Currently, up to one kilometre away. The IMSI Catcher does this by 'posing' as a mobile phone tower, tricking your phone into connecting to it and then revealing your personal data without your knowledge.

IMSI Catchers are surveillance tools that can be used to track people attending a demonstration, a public event, to monitor your calls and edit your messages or to pinpoint a target's location. Normally these tools are exclusively for state services, but I hope everyone has realized that this concept is totally outdated. I have made enquiries with various suppliers. I have either received no response or was told that it was not for me. No European or American supplier has sent me any information or offers.

The entry-level model, ethics can be bought on Alibaba, from 1500 dollars. You'd think that in a year or two, you could take a zero off that price.

20. The anonymous credit card

In the course of intelligence work, you will probably be required to make online purchases or take out subscriptions on certain sites. In this case, you do not want to be traced. Governments have long fought against these payment systems because they are traditional tools of terrorism and money laundering. You can very easily find a prepaid card, but since January 2020, anonymity is not guaranteed only up to a maximum of 150 euros.

If that's enough for you, no problem, you'll find them everywhere.

If your mission requires more resources, there are solutions. You can set up an account in places like Anguilla, the Bahamas, Fiji, Guam, the US Virgin Islands, the British Virgin Islands, Oman, Panama, American Samoa, Samoa, Seychelles, Trinidad and Tobago and Vanuatu. Banking secrecy is absolute. Please note that this list changes regularly. Once you have an account, you can easily obtain a totally untraceable credit card. Swiss establishments will promise you the same thing, but there is always a risk.
At Vadiance for example, you can get an anonymous credit card with funds from any bank. You will simply be asked for an IBAN.

http://www.vadiance-offshore.com/

In the first edition of this book, I provided a list of places where you could buy all these tools. Today, almost everything can be found on Amazon including the top of the range ones. Every product has customer reviews and that is a valuable advantage. These constant reviews have also put the suppliers under pressure. One poor quality device, one poor service, and that's it. Ten or fifteen years ago, if a customer wasn't happy, it didn't have much impact. With technical equipment, a negative notice does not mean anything. It is possible that the customer got angry without reading the instructions.

However, on Amazon, there is no explanation. If you need assistance, it is better to shop on a specialized site where you will be answered in English.

UK

https://www.spycatcheronline.co.uk/contact/

https://pakatak.co.uk/ (with a blog)

https://www.spyequipmentuk.co.uk/ (with a shop in Coventry)

https://www.euspyshop.com (with a shop in London)

Canada

https://www.thespystore.ca (shops in Vancouver, Calgary and Surrey)

https://www.spytech.com (shop in Toronto)

https://spytronic.com/en (shop in Montreal)

Australia

https://thespystore.com.au

https://spycity.com.au (shops in Brighton Le Sands and Southport)

https://www.securitylab.com.au

https://www.ozspy.com.au (with shops in the all country)

USA

https://www.spygadgets.com

https://internationalspyshop.com

https://www.spybase.com

https://spystorenyc.com

There are thousands of online shops. Avoid the ones that don't even give a contact phone number as they are often dropshipping sites that buy from Alibaba and then sell the equipment back to you. If you are not used to using the equipment, it is worth working with companies that have real shops, with real people who will e xplain how the equipment works.

VI. Detecting lies in a CV

Many recruiters, professional or not, rely on their instincts during a selection procedure. Intuition is nothing more than a projection of the self. Those who think they have a gut feeling are the most mistaken.

Two professional categories have a high rate of false CVs: executives and salespeople. It is true that if you are a bricklayer, it is particularly stupid to lie since your incompetence will be discovered in half an hour. The higher a position is in the company's hierarchy, the more time you will have to prove yourself. Which in some cases will allow you to acquire skills you didn't have in the first place.

I do not judge these lies. Some of my clients have decided to hire a candidate knowing that they lied on their CV. They did so knowingly. I once had a candidate who, before starting the interview, said to me:

"I might as well not waste any time. In my last job I was fired for serious misconduct and the serious misconduct was justified. Should I sit down or should I leave right away?

Like just about everyone else in my position I guess, I offered him a seat. To cut a long story short, his wife had left him and one night he came home from work to find that when she left she had taken absolutely everything, right down to the coat rack. He started drinking. Then he started making false visitations reports and caused an accident with the society car by being drunk.

I told this story to a lot of people. Everyone reacted the same way, "yes, it's not right, it's normal to get fired but, well...". The guy wasn't honest, he was smart. He knew I would find out anyway. It's a different feeling if the candidate brings it up or if I find out. He gambled on it and he won. The client just said 'if he can sell a serious fault , he'll break the house down'. Which he did.

I understand some candidates between lying and staying unemployed or in a job with no prospects, the choice is quickly made. You don't necessarily want to admit that you completely failed your studies, that you spent two years in prison or that you were bedridden with depression. Things have

totally changed now, but at the beginning of my career, candidates who chose to travel around the world for a year or two were very badly perceived. Of course they would invent jobs abroad.

If I can be empathetic, it doesn't mean I'll accept. If my job is to track down the bullshit, I will track it down.

Your company will spend thousands of Euros on a recruitment and selection procedure: advertising, recruitment agency, hours spent, tests and assessment, training of the new employee etc.

The procedure proposed here will take between 2 and 5 hours. It should be an integral part of the process for all candidates in the final selection phase .

Checking the factual elements of the CV is slowly becoming part of our practice. For some companies or recruitment agencies, the following is part of the usual procedure. Anyone who has spent time checking these elements has come across some outrageous stories.

1. Ask for the candidate's agreement

It is in the recruiter's interest to seek the candidate's agreement before embarking on a reference checking process.

Firstly, for legal reasons. If you work in a recruitment agency, most industry associations require their members to obtain the candidate's consent before going on the hunt. But if you are an intelligence professional or the person responsible for recruitment in your company, you have a strong interest in having this consent because if you damage the candidate's career by checking references, the candidate may turn against you.

The other reason is more practical. At the end of an interview, ask a question like "What do you think your former boss would say to me if I asked him or her how you got on?

You will observe a fleeting expression on the candidate's face, which may be:

- Fear/concern
- Anger
- Full of confidence

- Embarrassment
- Disappointment
- Surprise
- Nervousness
- Contentement

Most candidates answer that there will be no problem and that their former boss will give excellent references. This is the socially acceptable answer and the candidate knows very well that any other answer will be detrimental to the further selection process.

Some, however, will explain with an embarrassed look that everything did not go well and that it is better not to contact them. You will then learn that the candidate's departure did not take place under the idyllic conditions he or she explained to you during the interview. You have just saved precious time.

2. What references to ask for?

The only relevant reference is that of the former line manager. The HR manager is not totally useless, but you will only get a few factual elements here: confirmation that the candidate has worked for the company, job title, date of entry and date of exit.

Former colleagues, clients or suppliers are of little interest as they will have been carefully selected by the candidate.

For your own security, you should ask the candidate to sign a document authorizing you to check references. This document should include a list of names of former supervisors whom the applicant allows you to contact. If you are a service provider contracted to check the CV, you will have taken care to check that your client has obtained this written agreement.

3. What to look out for when asking for references

The following is a non-exhaustive list of situations where your recruiter's radar should start flashing:

- The candidate claims that he/she worked for a company run by a family member.

- The candidate does not remember the name of their previous manager.
- The candidate gives you the mobile number of their previous boss. This may be for your convenience or because a friend will pick up the phone at that number pretending to be the reference.
- The applicant's previous company has gone bankrupt or has been bought out. The verification will be even more complex if the company is located abroad.
- The previous manager has left the company and the candidate does not know where he/she is working now.
- The reference given by the candidate does not speak English.
- The reference lives in a country that will require you to call in the middle of the night.
- The manager is retired or deceased.

The above in no way means that the candidate wants to hide something from you. It is only possible. If one of the above situations occurs, you know that your full vigilance is required. I have always assumed that what the candidate says is true until proven otherwise. This is the difference between paranoid suspicion and benevolent caution.

4. Check the diploma

Many companies do not properly check that the candidate has the degree they claim to have. Often they ask for a copy of the diploma or even the original. This is a largely insufficient method, it is so easy to make or buy a fake today.

But this is where many candidates lie. Especially high profile ones. Several studies converge on the same figures: 20% of candidates for a high-level position lie about their diplomas.

The main lies are:

- Training that does not lead to a degree
- Attending school but not graduating

- Exaggeration of the level actually obtained
- Difficulty in assessing the level of the diploma through the use of complicated acronyms
- Pure invention of a phantom university
- Counterfeiting of a degree
- Fake bought on the internet

To convince yourself of how easy it is to buy a diploma online, I suggest you search "buy fake diploma" on Google. Now you know that if you need it, you can be a neurosurgeon next week.

There are only two reliable ways to verify this information. Either by contacting the school directly (by email or phone) or by looking to see if the candidate's name is in the alumni directory. I once came across an organization that had created several websites of bogus universities, with false names, false blazon etc.

When it comes to training abroad, it is sometimes difficult to understand the real level of the degree. For example, a summer management course at Harvard can quickly turn into an MBA. MBAs are particularly popular in the big lie market and the prestigious Harvard University seems to be a favourite with fraudsters. This is a big mistake, because Harvard University will respond within the hour to any questions about its former graduates. Sometimes you will receive a candidate with a degree from a university with a fancy name, but you have never heard of this English or American institution.

It could be: The University of New Castle, The University of Devonshire, Youngsfield University, Cambridge College of Learning etc.

There are hundreds of them. Most of these 'universities' don't even offer courses.

If your recruiter's alarm bells go off when you read the CV, here are a few techniques to check if that gorgeous gilded degree is the real thing.

1. British institutions have not been in the habit of issuing degree certificates in Latin for many years. The current certificates are in English.

2. Locate the address of the university. When you go to the university's website, you will see pictures of a wonderful and busy campus. When you

type in the school's address on streetview, you come across a garage or an empty lot. If the address given on the contact page is a post office box, don't bother going any further.

3. Check the phone number. Just copy/paste the university's phone number between " " on Google and you may find that this number is shared by 53 other universities (it happened to me).

4. Type the name of the university into Google to see if it is already in a list of bogus universities. If not, you will most likely find reviews on the school's reputation. If you don't find any, it's a very bad sign.

5. With https://lnkd.in/gJzCc_6Y , you will find the IP address of the site, its location (approximate and not super reliable) and also if the site was created last week for the purpose.

6. If you run the name of the university on Linkedin, and make a selection of people, you will see if there are people who graduated from that institution.

7. Finally, some of these scams use real university names and change a single letter. It is very easy to fall into the trap.

5. Background checks

In some countries you can easily obtain the applicant's criminal record and this is legal but in most countries you cannot legally access them. Of course, you can always ask your old police friend for a small favour, but it is always risky. In France, leaders have been convicted for this. The first verification tool is Google. You type the first and last name of the candidate between " ".

You will be able to find photos, videos, documents, registered patents, newspaper articles in which the candidate's name is mentioned. There are many techniques for refining your searches via Google, but I imagine that for a verification of an application, it is not essential to carry out a real in-depth investigation.

You may also want to take a quick look at the candidate's Facebook profile. The purpose of this is not to obtain information about the candidate's private life.

If you find a photo of your future marketing manager dancing shirtless on a table, it doesn't tell you much of anything useful. However, if you find out from a press photo that he or she has been taken into custody, it's worth looking into. Just like if you find a message on his Facebook wall, congratulating him on his new job with your main competitor or his interventions in white supremacist forums or blogs. You may also find any factual element that contradicts a significant element of his CV. How often do you find this sort of thing? Not often but good enough to check systematically.

You should also check with the commercial register to make sure that the candidate does not run a company that he/she forgot to mention. Even if this is the case, it is not necessarily prohibitive, but it is still important that you be informed.

6. Contacting a reference

The contact with a reference given by the candidate is made by telephone. It is very rare that a person refuses to talk to a recruiter on the phone when it comes to a reference check. I have often seen recruiters doing reference checks by email. You might as well not give it a try. Often, you will not even get a reply.

If you attack directly with a question as vague as "I would like to know how the collaboration with Mr. X went", you risk embarrassing the respondent and getting an answer as rich as "it went well".

To start off smoothly, you check the purely factual information:

- Job title
- Date of entry
- Date of leaving
- Job content
- Reason for leaving

With this alone, you will not be short of surprises.

If something bad did happen, the respondent will not wait for a question to be asked before unpacking. But even when the collaboration went badly or ended badly, many respondents are reluctant to talk about it spontaneously.

For example, if the candidate is applying for a position where he/she will have to manage a team, it is better not to ask "how was Mr. X as a team manager?" but rather "what would Mr X. have to improve to be a better manager?" Or "in what kind of role do you ideally see Mr. X and why?"

I guess I'm not telling you anything new by pointing out that we are in the register of opinion here and not the fact. It is certainly interesting to have the ex-manager's opinion, but it is very subjective. You don't know and you will never know what happened between these two people. When you are lucky enough to be able to check several references and the comments are in the same direction, you may think you are getting closer to the truth.

Once I was checking the reference of a salesman and his former manager simply said "tell him he can come back whenever he wants". I think he got the job.

7. Case study

a) The candidate claims that he worked for a company run by a family member.

- Ask the candidate to present pay slips
- Ask the manager of the company the questions in point 6. Your family member will certainly be willing to claim that you worked in his or her company, but this does not mean that he or she will have planned an elaborate lie.

Let's be humble, in this case there is not much you can do. Asking a friend or family member to act as a reference is virtually undetectable, unless you conduct a thorough investigation. I admit to having done this for a friend.

b) The applicant's previous business went bankrupt or was taken over.

- Check that this is true for the dates mentioned by the applicant
- Ask for the name of the former line manager and the same as point 6.

c) The previous manager left the company and the candidate does not know where he/she is working now.

- Check that the information is correct

- We are in an age where most managers and executives leave a trail on the web. You should be able to find him/her quite easily via social networks

d) The candidate is still working and has been working for the same employer for several years

Of course, you cannot check the candidate's references without seriously damaging them. However, what is very easy to do is to check if this is true. Indeed, many candidates who have lost their jobs choose to lie about it. This is understandable, as a working candidate is more valuable to an employer.

The easiest way to do this is to contact the company in question by phone and ask to speak to the candidate. If you hear "I'll put you through", hang up.

For the record, I have been told several times in this way that the candidate not only does not work there, but has never worked there. Once this step has been completed, you have confirmation that the candidate is still working, or not. If the information is confirmed, you should at least know if they are doing the job mentioned in their CV.

Often you will find this information on the company's website. If not, if the candidate has said that he/she is a production manager, you phone the company and say that you have to send an e-mail to the production manager, "is this Mr. X? While the technique is a bit twisted, it still has the advantage of giving you very important information without harming the candidate and honestly, it is common for candidates to invent functions and responsibilities. It is the most common lie.

Last but not least, the ideal verification procedure should include the last candidates in the running for the job. Either you do it systematically, or you are sure to get screwed. Companies that do a "when in doubt" check are the ones that won't detect good liars.

VII. KNOW EVERYTHING ABOUT YOUR COMPETITORS

"Business is war and war is business". This quote is neither the work of a great warrior nor of a business genius, but of Kevin Anderson, a science fiction writer. I don't have an opinion on the second part of his sentence, but I agree with the beginning of the quote. Business involves competition between competitors. The strongest, the fastest, the smartest, the best adapted, wins. Unlike in real war, the loser or losers do not die. They lose market share and then sometimes rebound, sometimes disappear. The key to modern warfare is intelligence not merely sending 10,000 guys with bayonets to assault an enemy position, without knowing what awaits the soldiers when they arrive which in most cases is the worst.

Until the 20th century, spies were despised before becoming the heroes of modern conflicts. The business leader who does not care about his competitors is like those generals of the past who sent their troops to be slaughtered in the name of honour. The difference with war, and I am glad of this, is that when your company has collapsed because of lack of foresight, you will not die at least not physically.

In the previous chapters we have already seen various tools that are useful for competitive analysis, so there is no need to repeat them. A short summary will suffice:

- Boolean search and Google Hacking
- Google images and photo location
- Google video
- Google Alert

We will see in this chapter that private intelligence is divided into several branches. As far as we are concerned, our work will focus on two main areas of intelligence: HUMINT and OSINT i.e human intelligence and open source intelligence.

1. Human intelligence to know everything about competitors and (future) partners

According to the CIA definition, humint (human intelligence) is simply any information obtained from human sources. The methods used concur with other sources of intelligence. They are either a complement to them or the last resort when all others fail. Human intelligence is the most complex and expensive of all. These operations can be legal or illegal, some of which require the creation of a scenario. Human intelligence also includes the areas of social engineering, i.e. techniques for obtaining information from your target without them realizing it.

Social engineering is all about manipulation. When you hear on TV that an executive has wired a large sum of money from his company because he was tricked on the phone by a swindler, you say to yourself "what an idiot, it's not possible to be that stupid!

You are absolutely certain that it would never work with you. As a psychologist by training, I have taught manipulation and influence behavior in large Belgian and French companies. I know, it's not pretty, but it's a lot of fun. 100% of the participants were convinced that others could be manipulated, but not themselves. What makes manipulation techniques work is the belief in humans that they are ineffective on them. This belief in our strength is our first weakness.

You have to have an unusual strength of persuasion and self-confidence to convince a human to do what you want. When you walk down the street, people are surprised that the pavement doesn't stick to your soles because it is so obvious that the street belongs to you. You are never surprised or taken aback. We will see later that empathy, listening and timing are essential skills of the field agent.

Here we will look at a series of techniques for obtaining information from human sources. Some of these are very simple to implement, others require a great deal of skill complex implementation.

It depends on how much energy you, or your organization, are prepared to put in to get what you want.

It is also important to record as much of this information as possible when you collect it. Not only to document the evidence, but also to eliminate personal bias. As an exercise, sometimes attend a one-hour meeting, record it, and a few days later try to write down the key elements of what you

heard. Then play back the recording and write down your memories yourself.

For each of these activities, a briefing before the event and a debriefing afterwards is always an important part of the process as some team members may have picked up a nugget that others missed.

Passive listening

The least effective and easiest to use technique on our list is passive listening. The passive HUMINT listener is a sponge, absorbing all the information from any voice in the room.

Passive listening is practiced in public or publicly accessible places where people who could provide you with information are visiting like a bar, restaurant, trade show, airport or company cafeteria if it is easily accessible.

Unlike other human intelligence techniques, this one doesn't require much skill, except for patience. On a Friday evening after work, the employees of the company you are spying on go to a bar for a few drinks. Logically, you would think that in this day and age, when security is such a regular topic, executives would keep a low profile. Not at all. The Friday night drink is an opportunity to get everything that's wrong at work, out of your system and that's just what you're interested in!

Not long ago, I worked for a company that is classified as a 'defense secret' and is linked to the arms industry. I was there to run training courses. That's when I realized what the real weakness of companies was when it came to espionage. Just to get my foot in the door, I had to go through a whole process, including being validated by the intelligence services. Then I received a badge that identified me as a visitor and that I had to wear even in the toilets. Finally, someone would come to pick me up in the morning at the reception desk and I was accompanied every time I went from one building to another, without exception. Going from one building to another required a badge and mine did not open any door, except for the training building. If I had to change buildings, I had to ask for an attendant, who always arrived quickly and with a smile because, in addition to being competent, these people were friendly. In terms of technical and procedural aspects, this company was an example because, despite the cumbersome safety procedures, the pace did not suffer too much. The flaw was in the company

restaurant where I ate every day. People talk, It's normal, they laugh at the failed tests to decompress.

They laugh gently at the clients and express their hopes that contracts will be signed with this or that country. If I had been an agent, every lunchtime would have been a big harvest. The human factor is always the weakest link in intelligence and this is very difficult to change because Europe in general is not very concerned about espionage threats.

Another strong point of passive listening is if you are looking for a long-term informant. You work in a business intelligence firm and having a finance official in your pocket would be very useful. This is very bad indeed. I can't imagine you walking through the corridors of the ministry with a sign saying "who wants to make ends meet? But if you go to the cafés around the ministry and listen to the conversations, you will identify the most demotivated civil servants, those who are angry because "nothing works" or better still, those who feel they are victims of professional injustice. It is this profile that is most likely to betray their employer.

Interactive listening

Interactive listening is a stage in the channel where the listener will ask questions, echo some of the information they have just heard, or empathize with the subject to get them to go into more detail. Questions can be closed or open-ended.

Interactive listening is never hostile, lest the subject become silent. The best approach is empathy and understanding. Interactive listening is also free in that the conversation takes the direction the subject wants to go. This approach also allows the operator to establish a rapport with the subject, including personal likes and dislikes.

This is where the job gets complicated because you have to be good at what you do. Once the passive listening stage is over and you have identified potential targets, it's time to get to work and make contact. Wrapping up an informant is not easy on a personal level as they will often be someone you have no sympathy for and may even be offended by what they say. Never mind, keep your feelings to yourself.

Of course, trying to bag a finance official is not the same level of risk as trying to bag a NASA engineer. If the official detects you, or if you miscalculate and make an offer that he declines, it will be of little consequence. He will probably do nothing, not report you and you will get away with a simple "no thanks". With high strategic level targets, it's jail time. When I was searching for missing persons, I sometimes needed the help of the police, which is strictly forbidden in Belgium. I kept it simple. I went into a police station and asked for what I needed with all transparency. I never did this for a jealous husband, but in the context of parental kidnapping, I did and not just once. Parental abduction is not a priority for the police because the child is not in danger. So sometimes the family hands over the investigation to a private person.

When I arrive at a police station with this kind of story, what do you think a policeman does? He helps me by taking his risks not mine. Half of the policemen accepted. Those who refused always took the time to explain to me why, and very often it was because they had already been rapped on the knuckles by the hierarchy in a similar story. So there is no scandal, no denunciation to the Ministry of the Interior and no handcuffs.

The interview

The particularity of the interview is that the subject is well aware that he is being asked questions, with the answers expected of him. You can't just barge into the office of your main competitor's managing director and ask him questions.

You need status or what the spies in our beautiful countries call a legend or a cover. Unlike the intelligence officer who has to have total cover on all aspects of his life, you will only have to lie about a part, more or less important. In any case, if you are found out, the consequences will not be comparable to those experienced by an agent when the Iranian police come to arrest him at 3am.

We will look at some jobs where you would be legitimate to ask questions to your target.

The fake recruitment agency

This is really an elaborate spy operation, although it is still easy to carry out, especially in our countries where industrial paranoia is not the rule.

If there is one place where everyone talks, it is during a selection interview.

I am well placed to know this, because before practicing this beautiful profession, I used to recruit for the most beautiful companies and I have about 5000 selection interviews to my credit. Well, after this perfectly useless autobiographical digression, but delicious for my ego (like everyone else, I like to talk about myself), let's get down to business.

You will only use this shady and totally illegal method in extreme situations, you must be seriously threatened to use it. Or you really want to learn about your target.

So, everyone talks. Not under torture (I don't know, I've never tried it), not under duress, but voluntarily. Humans are made in such a way that in all of them, their favorite topic of conversation is themselves. Don't look for an exception, don't even think for a second that you are one, I said everyone .

The steps to follow are:

What do you want to know? Why do you want to know? Is such a complex scenario an effective way to achieve your goals? No, you won't improvise. Instead, you will take care to write an interview guide.
Who is your target ? Today, any executive's name can be found in two minutes on LinkedIn or Facebook. Alternatively, and this goes just as quickly, phone the company and say you have an email to send to the finance director, "can I have his name, please?".
Once you have the name of your target, you need to create your character. Fortunately, your caption doesn't need to be too complex. It must include:

A fake name. Make sure you choose your name carefully. The "candidate" may do a quick search on social networks. They will not find you. If you are not on Facebook, that's fine. But a recruiter who is not on LinkedIn is not very credible. Your name must therefore be assoc iated with a LinkedIn profile either because you created a profile or because you borrowed it from a real recruiter.

The name of a recruitment agency. This should be ideally one that exists abroad, in case the 'candidate' checks online, which he or she most certainly

will.

A telephone with a card, as you will need to give them a telephone number to contact you. Be aware that it is no longer easy to have an anonymous telephone, you will have to declare your identity. See the section on anonymous phones.

As the business card is no longer in fashion, you can dispense with it.

The name of a company you are hunting for. It too is located abroad, but the company is recruiting for the target country, otherwise the person may not want to come to the interview, as well as a profile of the ideal candidate, and of course a job description and a particularly attractive and realistic salary package.

That's it, everything is ready. You have your legend. You know the name of your target. All you have to do is bait them. Remember, you have nothing to sell. When you contact the target, you should of course be friendly, but above all sober. Don't put yourself in the position of an applicant, you will immediately be treated as such. A headhunter is always welcomed by a potential candidate. It doesn't matter whether they are interested in the job or not, they will be flattered. If you give the impression that you are trying to force an appointment, the target will be suspicious.

The next step is to contact the target by phone:

"Hello, Philippe Delval, from Human Research International, I work for an American (or Swiss or Belarusian) recruitment agency, do you mind?" And off we go. The rest is common sense.

On the phone, you do not mention the name of your 'client', real headhunters only do this at the first face-to-face interview. You don't talk about salary either. Instead, you make a promise of a position that is far superior to that of your target. The meeting place will be the lobby of a smart hotel. This is not unusual.

During the meeting you will be sober, correct, but not warm or friendly. You will start by asking general, uninteresting questions before you get to the subjects that really interest you. The target may hide behind the seal of confidentiality to avoid answering certain questions, which means that you have screwed up.

What if the target realizes that they have been tricked? In principle, that's okay, because they probably won't dare to say anything about it, especially if that good financial manager had a sharp tongue. There is a very small risk that a complaint will be filed. I hope for your sake that you have cleaned up after yourself.

Now I come to the last point: talent. If you have no acting talent, if you don't know anything about the world of recruitment, forget it, you won't succeed. Also, outsourcing this kind of work is difficult because it's all very illegal, although trickery is a legal way to get information. Maybe you risk being sued for breach of trust, but I have a big doubt.

In any case, if you like this technique and you use it, it means that vice is in your blood. So, the law does not concern you anymore.

The fake journalist

The fake journalist uses many of the same tools and attitudes as the fake recruitment agency. Except that the legend is easier to create. Basically, you just need to phone your target and say that you are preparing an article for such and such a media and that you want to interview the target. You're playing on vanity and it's pretty rare that it doesn't work.

Honestly, if a journalist contacts you for an interview, how will you react? Well, we agree. Vanity, everything is vanity. You can use the name of a real journalist in case the target checks, which is highly unlikely, but there is a risk that the target will find out that this journalist has no intention of interviewing you at all. Better to use a fake name, which is always one less crime, and in case the target checks, say that you are a freelance journalist.

As you are really a forward-thinking person, you take the precaution of buying a fake press card on the net but no one will ever ask you for it.

https://www.idcreator.com/ will be happy to make you a real fake at a very low price.

The method is simple and easy to set up, much more so than the previous one. One problem with the journalist scenario is that TV has taught us to be wary of the press. As much as an executive who is a little frustrated, as they often are, will speak quietly during a recruitment interview, he will be cautious with a journalist, since he knows that what he is going to say will be published. So forget about trade secrets and other merger/acquisition plans.

The fake client

This spy scenario is very broad. It depends on both what you want to know and the context of your target. We will therefore look at a series of applications and their respective methods.

Mystery shopping is a very fashionable marketing tool in recent years. It consists of sending a fake customer to evaluate your own services, either those of the salespeople in the field (especially in-store salespeople) or the telephone reception. In this version, it's about spying on yourself in order to test the skills of your employees. All companies that use this method warn their employees that this operation will take place. On the one hand, to avoid problems with the trade unions, and on the other hand, because knowing that they are about to be evaluated, the employees give their best during this period. This is both an intelligence and a management tool.

I carried out an assignment of this type for a client who owns a chain of high-end clothing shops. The results were dismal in almost all the shops. The reception was non-existent, the staffs were glued to their mobile phones, they didn't listen to the customers, etc. Everything was bad. The client was initially furious, but then organized a meeting with all the staff, soberly describing the results shop by shop. I saw several employees start to cry. The client remained calm, did not lose his temper with the staff, and made no threats. Three months later, we did it again, not with the same fake customers of course, and the results were spectacular in terms of progress.

Mystery shopping can and should also be used with your business partners, to check that your distributor is not talking rubbish about your products and also to find out if this distributor is effective in marketing your products. For example, does your distributor spontaneously talk about your products when a customer is looking something close to your range?

What I suggest, to enrich the information, is to conduct the same mystery shopping at your place as at the competitor's and compare the results. The most basic level of the fake customer scenario is still to call the target by phone and ask questions.

This guide is still about sending a fake customer, but this time you send him to your competitors again, with a good scenario worked out in advance.

What you can learn from this mission is close to what you can get at a trade show, with the added bonus of the responsiveness of the in-house team.

There are situations where this method is relatively easy to use. When your competitor:

- Sells its products or services via publicly accessible shops.
- Sells its products or services to private individuals.

If it is easy to go and study your competitor who sells fitted kitchens or leather lounges, there are many trades where the tradition implies that the salesman has to come to the shop: swimming pools, verandas, window frames etc. Here, you will use the home of an acquaintance or one of your salesmen and bring your competitors in one by one. In a few days, you will know absolutely everything about the strengths and weaknesses of your competitors, both in the technical and human fields. One of my favorite clients has compiled a well-documented book, updated every year, of which each of his sales representatives receives a copy.

If your competitor is in the B2B business, you can assume that his salespeople are used to visiting customers in their company. As it is not feasible to have the sales staff of the competitor at home, you have to find something else.

Basically, you have three options:

(i) Either you come up with a credible idea that allows you to host

this salesperson in a public place, such as a hotel, but if it's too unusual in your industry, the salesperson will be suspicious.

(ii) Or you use someone else's business, a friend or a client (to whom you give a small gift, it maintains the friendship) to receive the sales representative.

(iii) Or you explain to the salesperson that you would prefer to come to his or her premises, to see who you are dealing with.

Sometimes the job can be done simply by phone, especially if all you want is to receive an offer. In this case, if you are in B2B, you don't have much choice, you will need the complicity of someone working in another company, who will receive the offer without arousing attention.

Up to a certain level, this is very easy and does not require much investigative skill. The pinnacle of the fake customer scenario is to manage to get invited for a tour of the competitor's facilities.

I never practiced the following scenario, simply because I didn't need it. But a colleague and friend used it regularly because he specialized in physical intrusions. His clients paid him to test their security level. He could have a field day because if he got caught, he didn't risk anything. He had a whole series of victory selfies where he would take a photo in the office of the managing director of the company he was to test.

In short, if you want to visit your competitor's facilities and production sites, a simple phone call will not suffice, nor will an email, however well crafted, from your gmail.com address.

Let's take an example. Your competitor is a manufacturer of industrial pizzas. You know that he has developed a new production line that allows him to triple his capacity. You would like to visit his facilities, but you know that a simple polite request may not be followed up. It's vital for you to find out more because your colleague's prices will plummet and you may find yourself thrown out of the supermarket.

You have two options: either that of the big potential customer or that of the supplier who offers an exceptional opportunity. The second option is both more complicated and uncertain because even if you offer Gruyere cheese for 30% less, you can't be sure of being invited but if you represent a Dutch retail chain that is about to set up in France or Switzerland, you will

certainly be welcomed with open arms. And while you're at it, use the name of a real Dutch group.

However, you will need a credible website. You can create one in two hours with www.one.com or www.wix.com. You will need to enter a valid email address to register. I don't recommend using an existing address as you will leave a trail and today, industrial espionage is a major irritant for the authorities.

That's why you create an email address on https://mail.yandex.com/ which is not untraceable, but which severely complicates things. Alternatively, you can get a temporary, anonymous, disposable email address from a site like http://www.yopmail.com/ and this email address will self-destruct after a few days.

Ideally, you keep the same domain name as the Dutch group but register it with a ".fr". There is a 9 out of 10 chance that this will not work because the name will certainly have been registered by the Dutch group. You can still try. Otherwise, use a name that is fairly close and write on your site "member of XXX group". With your new site, you get a credible email address because it has the same name as the site itself.

Before contacting the target audience, you will have taken time to write a specification that makes sense. It must be feasible since it is your competitor.

Then, exchange emails and phone calls. You don't use your personal phone of course, we saw that in another chapter. You will also need a spy camera. This is covered in the chapter on equipment.

What is really tricky in this mission, which up to now is rather simple to do, is the choice of the person who will do the visit as I don't see you doing it yourself very well. You have to find someone who is very credible, confident and who "goes down well" with the company director, who will probably make the visit himself.

When I started working as a private investigator, I was very successful in companies. I would have liked to think that this was because my skills were far superior to those of my colleagues, but this is not the case at all. In fact, when I started out I was probably much less competent than most other private investigators though I spoke the same language as them. We were

from the same world and that's something that's very difficult to emulate. I had run a company myself for 15 years, it was a relatively well-known company, and without any logic, that was enough to make me a credible person to investigate. In this "intrusion" scenario, credibility will be the determining factor. This credibility will come from the control of your character, but also from the questions you ask and your attitude too. Retail buyers are not known internationally for their kindness of spirit. Finally, you will need to practice using your camera beforehand so that you don't have to handle it during the visit.

After the visit, you have two options. Either you simply stop answering the industrialist's emails and he will take this as a lack of interest in the collaboration or you can close the site and delete all traces. In the first case, the disadvantage is that the site remains online for too long and the genuine Dutch company could get to know. In the second case, your pigeon will know that it has been duped and may file a complaint. Probably there is still another way to get into the factory, and that is to get hired as a temporary employee. This is the perfect solution because it is the least risky and least binding, but how long before a position becomes available is not certain.

The notary's office

At the time when I was mainly involved in the search for missing persons, I considered that it was my job to search until I found something. I was exclusively in a hunter's mindset, which I must admit, corresponds quite well with my temperament. But this logic, as exciting as it is, is time and energy consuming. By chance, I came across an American article about an FBI operation. They sent thousands of Americans wanted by the law a ticket each for a free week on a cruise ship. The prize tickets were sent to the homes of the wanted persons or their families. The majority of the fugitives did not show up at the port, but several hundred of them boarded the authentic boat provided for that purpose. This made me think that trickery was cheaper than hunting and I started to think about how to get people to come to me who, on the face of it, had no desire to talk to me, let alone see me.

I started to regularly approach the family of my targets, claiming that I worked for the office of the notary XXXYYUV and that I had to be able to speak to Mr. Target or at least have an official address because I had very

important documents to give him. I never said that there was a large inheritance.

It was unnecessary. As much as we associate the word "bailiff" with "trouble ahead", the word "notary" will be freely associated with substantial gains ahead. Of course, people would ask me questions on the phone, and each time I would reply that it's confidential, that I can only talk about it with Mr. Target, "but you can imagine that if a notary's office calls..." without ever finishing my sentence. Imagination is always stronger than argument.

I would like to make it clear that I was not tracking down criminals. I was either in the context of family stories or in the search for indelicate debtors. Not people who are suspicious of their own shadow.

The notary scenario was a hit. It has just one drawback, it is totally illegal. I avoided falling into the usurpation of a protected title by saying that I worked in a notary's office. I never said I was a notary. I don't know what I was risking, I was never worried.

The false candidate

This is the worst scenario. That's it. If your target is recruiting, it is very easy to come up with the perfect CV to be invited to a selection interview. But if it's for a high-end position, you won't get any information at all, as you'll probably be interviewed by a professional recruiter who will be unable to provide you with any substantial information. If the recruitment is conducted directly by your target, you may be able to get something out of it as in this type of interview the recruiter talks 80% of the time.

But I think that's a lot of energy spent for less. I quote him anyway because in fact the limit in human intelligence is your imagination and your ability to organize it.

Guile is a very limited method of investigation in legal terms. Inventing an identity is not identity theft, but impersonating another person by using their name or worse, an official identity, is not to mention a breach of trust.

I am not a moralist, I repeat, it is up to you to draw the line. For the record, even if I'm not a saint, I've never taken a false official identity. It's too dan gerous, too risky and useless.

2. Detecting the lie

In human intelligence, lie detection is a high-value weapon. Everyone lies, sometimes to protect the integrity of others ("what are you talking about, those trousers don't look fat on you at all.") and therefore, they are minor lies. Intermediate lies are those that are told to gain an advantage, while the most serious level is covering up crimes and offences.

Many people are convinced that they can't do it to themselves, that they can spot liars at a distance but in reality are surprisingly bad at detecting lies. One study, for example, showed that people could only detect the lie accurately 54% of the time in a laboratory which is impressive when you consider that the detection rate is 50% by pure chance.

Since I can't remember the sample size, it's even possible that the 4% is just the margin of error.

As I am a proponent of the least effort, I have been interested in the technological aspects of lie detection for over 20 years. Indeed, if a machine can do the job, why bother developing skills? The technology exists, and it's not even new. It's even getting better every year. You can find lots of apps today that install in the blink of an eye on your phone.

The **polygraph** was invented over 100 years ago. What could be more logical than to imagine that lying causes excess sweating that can be measured? But sometimes the polygraph can be fooled by several factors. Taking a painkiller, biting your tongue during testing or simply going through an unsettled period that puts you in a stressful situation that cannot be measured.

The **Eyedetect** from Converus is an instrument that seems to be largely reliable. EyeDetect measures changes in pupil diameter, eye movements, reading behavior, blinking etc.

But whether it's an app (mostly used for jokes), the polygraph or any other measurement tool, it's all about getting the respondent's consent. The reader of this book, whatever his/her job, works in private intelligence, where you have no authority over the person being interviewed.

You can't easily ask a person to log on to a machine, although this is done in some security recruitments. I can't see myself asking the future European

marketing director of a large food group to submit to this kind of thing he will certainly refuse.

The same goes for a private detective who asks questions of someone who can lead him to a lead, or better still, a company director who asks questions of his competitor's salesman in order to extract information from him.

An intelligence professional must have a good level of non-verbal behavior analysis. What worries me is that some people think it's just bullshit. Usually, it's those who haven't given it much attention. So it's something you learn. The good news is that it can be learned quite quickly from a few days to a few weeks to get to a very respectable level and acquire skills that will make you show off in the finest cocktails.

Why it is quick to learn is because it's about learning a new skill not replacing one. I realized this when I started running this kind of training for a major bank, for lawyers and private investigators. At the end of a single day, the progress of all participants was phenomenal. Whereas when I conducted training in non-directive interviewing techniques, the results were far less convincing. Everyone thought they were good listeners.

But you can do it without:

- Interrupting the speaker
- Asking closed questions but mainly open questions
- Making judgements
- Giving opinions
- Giving advice (which absolutely nobody ever follows)
- Talking about oneself
- Neglecting to show empathy and being able to rephrase to show understanding

It's complicated because it doesn't come naturally to most people. The participants agreed that, genuine listening takes these criteria into account, but almost all of them were used to doing it differently. In this case, my course was a re-learning.

Are there any techniques to detect lying for sure? Not at all. With that said, let's move on. One last thing: many people who are ill-informed about the analysis of non-verbal behavior make the same mistake. What

psychologists call the over-attribution bias. This means drawing broad conclusions from observation of a single phenomenon.

To put it simply, just because someone crosses their arms does not mean that they are closing themselves off. A convergence of elements is essential.

A) Detecting lies through verbal methods and questioning

Ideally, you should be able to see the whole body of the person and therefore he/she should not be sitting behind a desk where a large part of the body is hidden.

During questioning, professionals who can, often place the subject in a chair in the middle of the room so that they can look for clues to deceptive non-verbal behavior. Of course, you do not want to appear to be interrogating the person, but it is often best to have no object such as a desk or table between you and the other person or to sit in a neutral place where you can observe the other person's entire body language, for example on a couch, which is comfortable, relaxing, and allows you to see the person's entire body.

When you ask a suspected liar questions, there are verbal cues that many liars give away. Here's how to tell if someone is lying to you by spotting 7 clues to verbal deception.

1. They repeat your question before answering - This is a common blocking tactic liars use to fill in dead space, while their mind tries to formulate a response that is consistent with what they have said previously. Repeating the question is not necessarily proof of a lie. The question may simply be uncomfortable.

2. They respond with a 'fog' question - A fog question is when you ask a question back. An example might be "Why are you asking me this question?" or "Why are you asking me this?"

3. Responding in a guilt-ridden and aggressive manner. An example of a guilt-inducing statement is to say something like "Are you interrogating everyone?" "Do you really think I would be able to...?" If this is accompanied by an increase in aggression, it is a strong indication of lying. The caricatured image is that of the man suspected by his wife of che ating and who lashes out with "Do you really think I would be capable of doing

that to you?" because a man who does not cheat on his wife will rather seek to reassure her.

4. Respond with a justification. The person does not answer the question but explains why they could not have done what you suspect them of doing. Justification is an explanation that no one has asked for. The principle of justification can be used to turn a liar. A long time ago, I read an Australian criminology study. This study highlighted an interesting effect of the projection mechanism. When police officers asked suspects in a robbery "What do you think should be done to the person who robbed the house? », the guilty ones found extenuating circumstances and went into empathy mode. While the innocent subjects almost always said that the thieves should be severely punished. In short, if you suspect someone of something, ask them this question. It's a trick I've used for many years and often, in my head, I thank the Australian police.

5) Answer in too much detail. When someone thinks you suspect them of lying, they will always try to give you the best answer that will corroborate their story. This takes a lot of mental energy. However, when a person lies, they often exaggerate their story in the hope that by providing more details they will prove that what they are saying is in fact true.

6. Respond with distancing statements - A distancing statement uses pronouns rather than a person's name. Consider the statement made by President Bill Clinton when he said "I never had sex with that woman". By using "that woman" instead of Monica Lewinski's name in the original statement, Bill Clinton was distancing himself. Liars tend to distance themselves by deleting the "I" or by not using a specific person's name in their answers. The use of distancing statements is often an indication that a person may be lying about something.

Another form of distancing is to answer in terms of values rather than a specific fact. Saying "I would never steal the trunk of a church" does not have the same meaning as "I did not steal the trunk of this church".

7. A story has a preamble, a main event and an epilogue. When someone spends little time talking about the main event, such as stealing property or falsifying data, and spends more time talking about the elements of the preamble that led to the event, this may be a clue that this person is lying.

Another clue used to tell if someone is lying is that liars tell their story in chronological order, whereas sincere people usually tell the most intense part first. Only then do they complete the story with supporting details.

To trip up a suspected liar after they have told you their story, ask them what happened just "before" something, as this kind of question breaks the chronological order and makes it harder for a liar to stay on track. This is because a lie is a compact block, unlike reality. This trick is great in selection interviews. It's about letting the candidate speak without interruption before asking something like "and before you left X, what happened?" and you'll immediately see people get confused because a fabricated story doesn't get told backwards. Just a little neurological problem.

In the case of the cheating husband, it would be asking him to tell his story from now until the beginning of the evening. But you already know he's going to get mad, and dig himself in even deeper.

B) Detecting lies through eye movements

When we answer questions, we look for the answer in our memory and this can be seen in our eye movements. These eye movements are different depending on the type of information you are going to search in your memory. From this easy to establish and verify fact, many people have come to the conclusion that eye scan observation is a fantastic lie detection technique. Unfortunately, it's not that true. Let's say it's not wrong, but to make it, as NLP (neuro-linguistic programming) claims, an absolute tool is totally absurd.

When a person looks to the top right before answering a question, most of the time it is because that person is looking for a visual answer constructed in their imagination. This has been associated with a deceptive answer and is probably often true, but not always. Intelligence is about subtle people and two-bit generalities will never make you an elite spy.

You can observe that often when a person looks up and to the left before answering, they are searching their visual memory and therefore remembering images from their memories and that is what has been associated with the truth.

A person whose gaze sweeps to the right is creating sounds or noises. It's in their imagination. Test it on yourself, and you will immediately realize that your eyes do not go in the same direction when you remember a song and when you compose a tune yourself. The sideways scan to the left is therefore associated with the recollection of auditory memories.

Looking to the right is often linked to the imaginary creation of kinesthetic sensations, i.e. touch. Conversely, leftward gaze is related to kinesthetic memories or internal dialogue.

Mastering this technique is a good way to learn to detect certain lies, or at least to have elements that suggest that my interlocutor is or is not sincere. However, there are some biases.

The first is that this kind of gaze mapping is very far from being an absolute truth. The above is true for the majority of the population, but not for everyone. This means that to be sure of drawing relevant conclusions, you will have to ask your subject control questions, the answers to which you know, in order to validate their personal mapping.

The second bias is that untrained people tend to ask closed questions. That is questions where the answers will be binary. Yes or no, right or left. To be able to detect eye movements, you absolutely must ask open questions that require your subject to do a genuine search of his or her hard drive. If the questions are closed or too simple, you will not see anything at all.

Finally, it is very difficult for the average person to pay attention to a conversation and to watch the subject's eye movement carefully. In a perfect world, you could film your target from the front during the interview and study the video afterwards. The key is practice and I suggest you test your

loved ones s paringly if you don't want to end up, as I did, with your other half wearing sunglasses for breakfast.

C) Detecting lies by observing non-verbal behavior

On a Monday morning, you arrive at work and see Matthew. By reflex, you ask him if he had a good weekend and he answers "yes, not bad" by shrugging his right shoulder. Intuitively, you know that he didn't have a great weekend. When a person says something and simultaneously raises their right shoulder, it almost always means that the truth is the exact opposite of the words spoken.

Welcome to the study of non-verbal behavior. It is indeed very easy, you have done it thousands of times, to lie with words. But making your body lie is much more complicated, if not impossible over a long period of time.

Part of the analysis of non-verbal behavior is the expression of emotions on the subject's face. This is an essential part of the work of psychologist Paul Ekman. He determined that there are 8 basic emotions and that they are universal and genetically determined, and therefore that culture has an impact on the way emotions are expressed, but that overall, the basic characteristics of the expression of an emotion are universal. These emotions are:

- Fear
- Anger
- Joy
- Sadness
- Contempt
- Disgust
- Surprise
- Shame

This does not mean that there are no other emotions, but this short list represents the basic emotions, much like there are basic colours.

The point of being an intelligence worker is to be able to identify these emotions via facial expressions, and to identify what Ekman calls micro-expressions, which are fleeting expressions that are very revealing of your target's state of mind.

To become a champion at analyzing non-verbal behavior, you need two things: the skills to detect signals, and speed. The skills are acquired through learning and the speed through constant experimentation.

You can find a lot of videos in English on You Tube about this subject and how to practice. The problem is always the same: people come to conclusions too quickly. Observing non-verbal behavior is not an absolute science. With rare exceptions, you can't associate observed behavior with absolute meaning.

The keys here are humility and learning.

My recommendation here is to watch an American series "Lie to me". This is a series about the adventures of Dr. Lightman, whose mission is to determine what is the truth in civil and criminal cases.

I find the series exciting, but that's not what counts. It is a series where you will learn a lot about the study of non-verbal behavior.

D) The scintigraphic technique

You run an organization and you know that sensitive information is passed on to the media. Some people are likely to be responsible for this lack of discretion, but you have no idea who they are. Normally, you trust all of them. The scintigraphy technique is for you. A scan is a medical imaging method in which the patient is injected with a radioactive tracer, which allows the observation of a tumour. This is exactly the same principle employed here. If four staff members are likely to have spoken to the press, you tell each of them the same story, under the seal of secrecy, changing one detail for each of them. You can do this simultaneously or one after the other. The false detail is the tracer. When it appears in the press or as a rumour, you have your culprit.

3. How to inspire confidence in your target

By the time I wrote this, I had been living in Thailand for a few months. A few days ago, while walking in town I heard a man speaking French with an accent from my region. I spontaneously went up to him and asked him if he was from Charleroi, the town where I’m born. He gave me the smile of someone who had found his brother after years of searching. In two minutes

we were sitting down to a beer but if I had met the same person on the streets of my home town, none of this would have happened. So, we tend to feel comfortable with people we have something in common with. We feel good when with people who are like us and this is not an absolute statement but a tendency, and a behavioral tendency can always be used for various purposes, more or less benevolent. As benevolence is not the focus of this book, we will talk about synchronization.

Synchronization is the art and techniques of modeling yourself on your target. It could also be called the "chameleon effect".

It is possible to synchronize at different levels. Very good communicators do this partly spontaneously.

- On verbal language: speak in the same way as the target, adopt common words, have the same level of language.
- On non-verbal language: position yourself like the target, move like them, without caricature. If you scratch your nose because the other person scratches his or her nose, you will miss something.
- On values: having common values brings people together. On the other hand, a disagreement on values tends to drive people apart.

On activities: having a common hobby with your target will open the way to their affection. The risk is of course in being discovered if you know nothing about it.
On the para-verbal language: you speak at the same rhythm as your interlocutor. Talking faster than him/her will irrationally give the impression that you are haughty or aggressive. Talking more slowly, you will feel that you are intellectually slow. This is the rhythm of speech. You also match their pitch.

This technique is used by elite negotiators. Its use tends to relax the other person. This is not hypnosis, but a form of induced relaxation. Olympic champions of the technique are able to match the target's breathing patterns.

The second way to inspire confidence is to listen carefully to your target. You always like someone who listens to you a little bit. Let the target talk, feel passionate about his miserable career, show empathy for all the promotions that have been offered to his colleagues, of course, but don't talk

about yourself, he is not interested. Remember that you are never as exciting as when you say nothing.

Never criticize your target's choices or decisions, even if you feel like throwing up. Make him or her feel like the most interesting person on earth. Welcome to the intelligence "dinner party".

4. Manipulation for offensive intelligence

Human source intelligence and social engineering have in common that the human factor is at the heart of the operation. One thing distinguishes them, however: the purpose. The purpose of Humint is to collect information, whereas the purpose of social engineering is to attack and manipulate to gain an advantage.

Social engineering is the term used for a wide range of malicious activities carried out through human interaction. It uses psychological manipulation to trick users into making security mistakes or giving out sensitive information.

What makes social engineering particularly dangerous is that it relies on human error, rather than on vulnerabilities in software and operating systems. Mistakes made by legitimate users are much less predictable, making them harder to identify and defeat than a malware-based intrusion.

Social engineering attacks come in many different forms and can be carried out anywhere there is human interaction.

Thought hackers make prodigious use of weaknesses inherent in almost all humans: the belief that we are better than others (and therefore need not be careful) and the way we justify our failures by external factors and our successes by internal factors. Basically, I am only responsible for what I achieve. This is what psychologists call the complacency bias. Social engineering also uses other psychological factors: the need to help someone who asks for help because it is very difficult to refuse to give help but also the submission to authority, which means that the vast majority of the population obeys an order given by someone with an authority considered legitimate. Ego and greed will complete the list.

Phishing

Phishing is one of the most popular social engineering attacks. It consists of email, SMS or social network campaigns that aim to create a sense of urgency, curiosity or fear in victims. It then tricks them into revealing sensitive information, clicking on links to malicious websites or opening attachments containing malware.

An example is an email sent to users of an online service alerting them to a policy violation that requires immediate action on their part, such as a mandatory password change.

It contains a link to an illegitimate website - almost identical in appearance to its legitimate version - that prompts the unsuspecting user to enter their current credentials and new password. Once the form is submitted, the information is sent to the attacker.

Some campaigns are childish and hardly anyone falls for them. Others are much more elaborate and are not necessarily very difficult to set up. Let's say you have a subscription to the tarata.fr website and you receive an e-mail from tarata.be or tarata.it or .eu or tratata.fr, there is a good chance that you won't see anything wrong with it.

For example, I own the domain name agakure.eu, but I haven't bought all the potential domain names.

There are many sites that allow you to find out if a domain name is free. https://www.godaddy.com

Bait attacks

As the name suggests, bait attacks use a false promise to pique a victim's greed or curiosity. They lure users into a trap that steals their personal information or inflicts malware on their systems.

The most maligned form of baiting uses physical media to disperse malware. For example, attackers leave bait - usually USB sticks infected with malware - in prominent places where potential victims are certain to see them.

Victims pick up the bait out of curiosity and insert it into a computer at work or at home, causing malware to be automatically installed on the system. Bait scams do not necessarily have to be carried out in the physical world. Online forms of baiting consist of attractive advertisements that lead to malicious sites or encourage users to download an application infected with malware.

An example seen recently online: a site, obviously Indian, promises that for 50 euros, I would get a software that can download email addresses from LinkedIn, Facebook, and some other social networks. For 50 euros, I'd give it a try especially since the demo is very attractive. I already had my credit card in hand when I decided to check if the software had any comments. Fortunately it was a Facebook site but obviously brand new and without any comments, so I put my credit card away.

You'd think you'd have to be a high-flying hacker to pull off something like that. I can't believe that two days ago, when I was struggling to put a fan together, my girlfriend looked at me with the amused compassion we reserve for clumsy children. Of course I can't make this kind of software and if I use one that I find on the web, it will be identified by any anti-virus software for sure though any computer science student can do it.

Spear phishing

This is a more targeted version of the phishing scam, in which an attacker selects specific individuals or companies. They then tailor their messages to the characteristics, positions and contacts of their victims to make their attack less visible. Spear phishing requires much more effort on the part of the perpetrator and can take weeks or even months to set up. A spear phishing scenario may involve an attacker posing as an organisation's IT consultant and sending an email to one or more employees. It is written and signed exactly as the consultant normally does, deceiving the recipients into

thinking it is a genuine message. The message prompts the recipients to change their passwords and provides a link that redirects them to a page where the attacker enters their credentials.

To send an email from any address, whether it's your boss's or that IT consultant's, all you have to do is register on a newsletter platform. True, you have to sign up, but we've seen in another chapter how to sign up for a site with a disposable address or one that self-destructs after 10 minutes.

The purpose of these platforms is to send a message to a large number of readers. To do this, you have to write a text. Then you also have to upload a database of emails but the funny thing is when the platform asks you to enter the sending address. Some platforms ask you to enter the email address in question, and then you have to go to your mailbox to confirm that it is your address. Some other platforms don't do this and you can then send an email from any address you like. Imagine what you can do when you have the power to write anything from anyone's email. The YMLP platform allows you to do this so far. I suppose that could change.

https://www.ymlp.com/

http://deadfake.com/ is a site dedicated to sending fake emails. They say it's only for jokes though I'm not sure if they make everyone to laugh.

There are many of these and you can use "how to spoof emails" as a Google query to keep up to date. These emails are theoretically detectable as fake but you usually find out afterwards.

In any case, any server can be configured to send emails from any address.

Harpooning can also be done by telephone. The only technique is to be the champion of the pitch. One such scam was very successful in France, where an individual pretended to be the CEO of the company, called an employee in the accounts department and pressured the employee to transfer a large sum of money urgently. It takes a lot of time to study his role, but also the victim's profile.

In this kind of scenario, you have to be able to change your phone number. A blind call will not open many doors because you start the contact by creating mistrust.

The basic principle of caller ID spoofing is to change the information displayed on the caller's display screen. Some of the points discussed in this chapter indicate that we can use the argument of authority and/or commitment to influence a person. Having your manager's direct number on your screen raises credibility to its highest level.

But the caller could also be a colleague from another department, a service provider or a police officer.

You might think that this incredible technology is only for the intelligence elite, and it has been but this is no longer the case. Today, you can find spoof id sites anywhere.

If you have a smartphone, you can find lots of more or less free applications on https://play.google.com/ . "Fake Friend Call ” is one of them. The problem with these apps is that they can be great on one day and fail to work on the next day. You have the location, the keywords, you just have to be whoever you want on the phone. There are also voice transformers, but this is too much of a gimmick for me to mention in this book. But it is possible to imagine equipment that could transform your voice into that of someone your target knows. Actually no, you don't have to imagine it because it has a name, "deepfake".

Deepfake is a very recent technology that could be summed up as the art of totally transforming reality without it being visible. This can be done on a visual and/or vocal level. The first case I heard of was only in 2019 when a con artist managed to "borrow" the voice of a German CEO and embezzle a large sum of money.

Deepfake audio can be used for all sorts of purposes, ranging from entertainment to criminal activities. Most Deepfake audio applications are intended for entertainment purposes, but can also be used for more harmful purposes. The State of California has just passed legislation on this issue.

Voice cloning involves taking an audio file of any individual voice and using it as a source to create fake audio recordings. With only a few hours of source material (audio recordings of an individual voice), deepfake audio software is able to clone the voice for use.

It is not yet possible to find a system that would allow you to modify your voice live on the phone using the voice of a particular person. We're starting to find software where you can use the voices of famous people, and that's very compelling, or applications that allow you to modify your voice, but live cloning is not going to happen any time soon. At the rate things are happening, the technology should be available soon.

To conclude this chapter on social engineering, I have a question for you, a little test:

Imagine the following scene: you walk into your building, followed closely by a man in his forties. He wears a smart blue suit and pretends to follow you inside the building. Can you visualise the scene? It's fairly commonplace and something similar must have happened to you many times. What do you do?

a) You open the door with a big smile.
b) You don't want to open the door, but since he's right next to you, you don't feel brave enough to ask him any questions.
c) You politely ask him who he is visiting.
d) You don't ask anything at all and close the door in his face.

Most people will answer c). Test this around you. The wonderful thing about human behavior is that in reality we are unable to predict our own behavior because it depends much less on factors inherent in our personality than on the context of an event.

5. Spoofing an email address or sending an anonymous email

We saw in the previous point that it is possible to send an email very simply from the address of absolutely anyone. If I want to send a message to 100,000 people using Bill Gates' address, he will not be able to do anything about it. This method can of course have absolutely devastating effects, but it has a drawback. You can send the emails, but not receive the replies. Since you do not have access to the inbox. The person will be informed within a minute of the fraudulent use of his address in two ways: via the replies he may receive, and especially via the mails that do not reach their recipient and that bounce back before leaving an error message in the inbox of the person who sent the message. Of course, here the target has not sent any message, but now knows that someone has. There is not much they can do about it now as they do not know who you have written to on their behalf.

There are other ways to send anonymous emails.

The easiest way, if you need moderate anonymity, is to create an address for yourself via any free email service. There are lots of them, in lots of countries.

Nothing could be easier but here your address provider can identify you either via the information you gave when you registered, or via your IP address. Your target can also identify you via the header of the e-mail where your IP address is located.

At this stage, you have two options: use a VPN, which guarantees that your IP cannot be located, or use a "remailer". Basically, you don't send your email to your target, but to another server that does the sending. And if you are really anxious, you can double or triple your remailings but then you become totally paranoid, which is a major risk when you work in intelligence. A new address with a free provider, in another country than yours, accompanied by a VPN, should be more than enough. Choose a "no log" VPN, i.e. one that does not keep track of your browsing, or even your personal information.

If you need an address for a few minutes, https://www.crazymailing.com will provide you with one that will self-destruct after ten minutes. This is very useful for registering on a site in total discretion.

You can also use https://temp-mail.org/fr/

6. Going through the rubbish

If you are not quickly disgusted, you will find a lot of information in the garbage because you can go through your competitor's rubbish, but also through the rubbish of company managers.

In our unsuspecting countries, everything ends up as waste, and most of the time without having gone through a shredder first.

With a private individual, it's simple, you'll know his whole life, all their habits and very often his financial situation. In a company, it will depend on the negligence of the managers, which is often very great in our country.

But basically, you will find:

- draft contracts
- Photocopies of credit cards
- Drafts of plans, analyses, current or future projects

Either the information found can be used in raw form, or as a prerequisite for a second step (if you find out that your competitor is about to sell to one of the big players in the market, this is the time to learn more about that player).

You should know that in some countries, a rubbish bin on the public highway...is public. This means that you have the right to search it, to take it, and that any information obtained by this means is considered public information.

The best thing to do for this kind of job is to come in a van, pick up the bins and open them quietly in a well-ventilated place.

Even if the method is unappetizing, it was a common practice among private detectives. For all our habits and many of our secrets end up in our bins. This is perhaps less true today, since many of our secrets are hidden in our computers. On the other hand, since it involves selective sorting, it is still more pleasant to only worry about the papers of our target, since it is what interests us.

In companies, everything is done on screen, but our habits have not changed much. We still print a lot. Printing means waste. In your company, does all the paper waste go to the shredder?

7. Contacting competitors' customers

If you want to know your competitor's strengths and weaknesses, the best thing to do is to ask their customers.

You can just read the opinions, reviews and other "reviews" that you find on the net. We'll talk about that but these online reviews have three disadvantages:

- It is mainly for companies that sell to individuals or in the service sector. Very few in the industrial sector.
- A very small proportion of consumers take the trouble to post a review.

- Only the extremes express their opinion. The very satisfied and the very dissatisfied.

The method to be used is simple and not very stressful. Here we are in an information-seeking process, not a prospecting process. The idea is to phone these companies and tell the manager that you are considering working with company X (your competitor), but are hesitant.

Experience has shown me that this approach is very effective because the people I talk to are very articulate. Our egos make us love the idea of someone asking our opinion, as it is both very rare and very rewarding. Of course, you have taken the precaution of not being identifiable, which is done, quite simply, by calling blindly from a mobile phone. Then the buyer will be happy to tell you all about

- The quality of the service
- The quality of the products
- The after-sales service
- Delivery times
- And of course, if you're a bit clever, the prices

I suggest that at the end of the interview you ask two open questions:

"In your opinion, what can be improved at X?

"What do you think works best at X?

This information is of paramount importance in a competitive analysis approach for e ither the approach will allow you to identify a major weak point in your competitor, and therefore to dive into their customer base or it is in your company that the weak point will be identified, and therefore you can improve it.

The technique described here is very simple, very easy to implement and requires no special skills or equipment. It is one of my favorites.

8. Fairs and exhibitions

Your competitors present their new products at trade fairs and exhibitions. It is your job to be there. As a company manager, it's rather tricky to pass yourself off as a customer at a trade fair. You risk being recognized, which is very embarrassing. Worse than embarrassment is the fact that if you are

recognized, there is no guarantee that the information you receive at the stand will be reliable.

In short, use the team.

In any case, a visit to a trade fair, like any intelligence mission, must have a purpose or purposes. Going out of curiosity is very nice, especially if you go with your family, but very unprofessional, unless you are in a sector that sells to individuals (in which case your family can be part of the scenario).

At a trade fair, you can get information on:

- Pricing (get a quote)
- Strengths and weaknesses of the sales team
- Technical innovations
- Delivery times, payment times, response times
- Physical identification of the competitor's staff
- What the competitor thinks and says about your company
- What is wrong with the competitor (salespeople love to complain)

Do not trust your memory. It will betray you and you will only retain what you want to hear. Record all your exchanges with a microphone that is both discreet and of good quality. Quality is important because a living room is a noisy place and you risk losing everything because of a poor quality recording. Never hide the microphone in your clothes, the creasing of the fabric will totally pollute the sound. Check out the section on spy equipment in or near your country.

If it is simple and safe, ask an employee of the company or a family member. If you are in an industry where a potential buyer needs to have technical knowledge, it gets more complicated. Either you find someone who has this knowledge or create a scenario that explains why you don't have it

Above all, never neglect your credibility!

You can get a real customer in exchange for who knows what. The best thing is your sales people. They go fishing for information and it is directly usable in the field. The problem with sales people is that they seem to have a strange disease that prevents them from passing on information to the marketing department. The problem is that like in your situation, they are

likely to be recognized. Experience also shows that salespeople have difficulty understanding the value of competitive information. They are reluctant to conduct simple "mystery shopping" assignments, while complaining that competitors are cheaper and more technically advanced than you.

If nobody can do it, ask a mystery shopping company. It won't break the bank. It's supposed to be their job. But that doesn't solve the problem if it is absolutely necessary to have high technical skills to be a credible client in your sector. Moreover, mystery shopping co mpanies fight a lot over prices as a result, mystery shoppers are often poorly paid and therefore the level is not there. Another solution is to use a sales training company. The trainers are used to this kind of mission when it comes to working at the top end of the market. The price will be heavily influenced by this. You can expect to pay between 600 and 1,300 euros per day but you will get a good deal.

Abroad

Where it gets really tough is when your beloved competitors show up at trade fairs abroad.

The first option is obviously to go yourself. This gives you a stress-free trip at the company's expense. It's expensive, just to spy on a competitor at a trade fair on the other side of the world but if the company doesn't plan to pay you for a holiday, another system should be considered. A system that I recommend you use if you plan to conduct constant and close monitoring throughout the year.

You must use local contacts. There are two kinds of contacts. Either you can use a local mystery shopping company or a private investigator (also local). Both professions can easily be found on the net or in national directories. This system allows you to track your competitors anywhere in the world, for an affordable budget.

These potential providers do not know you and vice versa. They will either ask you for the whole budget or a retainer. You can't escape this. If you use small businesses, it will be cheap and all surprises are possible. If you use a large structure, there will be no surprises, neither good nor bad, but the bill will be high.

If you need a special profile for this visit to a foreign trade fair, you have the world's largest network of foreign correspondents at your fingertips. I'll tell you the trick.

Register on an international dating site (Meetic). Then, do a profile search on the area in question. It will take you ten minutes to figure out how it works. The nice thing is that you can easily change your parameters. For example, if you are looking for someone living in the Stockholm area, you can change your profile by registering in the city of Stockholm. Then you ask to see all the profiles that live within X kilometres. You create your profile by specifying that you are looking for either a man or a woman. The number of profiles will be huge, so you can afford the luxury of asking for those who speak English or those who have a bachelor's degree if you want. Then you send a proposal in the form of a message to all the selected profiles by copying and pasting. The method is quite exotic and I have used it successfully. You will come across people who are a bit bored. If they are on a dating site, it means they are a little bored. The luxury is to find people who speak English, who enjoy it and who have a few hours to spare.

www.meetic.fr

Meetic is a French group with a large international presence. Each country has its own leading dating site. To find the one that interests you, type "dating site" + country name on Google.

You can try the same thing on Facebook, but it won't work as well because as you are not in the contacts of the targeted people, your messages might not be read. Moreover, you cannot select people by language, unless you go to a group of English-speaking expats, which can be a very good idea.

Don't try this with Tinder. On Tinder, you have to click on profiles that interest you and if that profile is interested in you, then it's a match. Unless you have a super-handsome profile, you might have to wait a long time before you find someone willing to help you visit your salon.

Me, I don't know why, I've kept all my affection for dating sites. Where you know that people are looking for something, even if it's not to play spy for you.

Don't forget to ask that person to record everything they do during the show.

9. Bribery

You want hot info? Buy it!

That's it, clear, direct and unambiguous. You can do this by bribing two types of targets:

- Finance officials
- employees or former employees of the target

This is regularly discussed in the press or on TV, especially with former executives, and I hate this method, again because it is too risky.

While it is likely that everyone is corruptible from a certain price, experience shows that the person who betrays corresponds to one or other of these criteria:

- needs a lot of money to pay for alcohol, drugs, debt, illness or whores (which can be cumulative).
- male, intelligent, over 40, has not achieved what he believes he deserves in his career.
- has developed a nagging grudge against his organisation (which justifies his future betrayal).
- Unlike some traitors in the field of state intelligence, you will not find any who will do it out of conviction. However, there are some who do it simply to get out of a colossal bind.

Recruiting a mole is a long and tedious job. Unless you know of a potential one in your immediate environment.

Be aware that if you ask someone for "a small favor", the worst that can happen is that they will refuse. And when that person refuses, they will do so out of fear of getting caught, not very often out of ethics. I can't see this person filing a complaint for attempted bribery of a public official.

This book is written for managers to use. I wanted to make it a working tool. If you have to start spending your afternoons in the favourite coffee shop of finance officials, hoping to make a contact, I am sure you will succeed and it's just as likely that the contact will end up giving you what you want but it's not an executive job. It’s too time consuming, very expensive, so random and terribly illegal.

10. Monitoring competitors' patents

A patent is an industrial property right that gives its holder an exclusive right to exploit the patented invention. This title has a limited duration, generally 20 years, or even 25 in the case of certain pharmaceutical products. The patent is only valid in a given territory. The content of a patent remains secret between the date of filing of the application and the date of publication. Eighteen months after the filing date, the patent file is published in full.

The chapter on competitive analysis is essentially aimed at marketing or sales. Technological or legal monitoring is not another job, just another specialization, which is not mine. I have been a consultant long enough not to be reluctant to talk about a subject I know nothing about, but it is something else to write about it and even worse to distribute it for a fee.

Checking your competitors' patents only interests me in this context. Where is your competitor, what is he doing, where is he going, are you behind or ahead? Nothing else.

I used to work for a law firm specializing in property rights. My tasks consisted of finding the rightful owners of a patent. Sometimes the patent had been registered for a long time and had expired. I must admit that I was tempted several times not to find the legal beneficiary and to take advantage of the non-renewal of the patent. I have never done this because I am a good boy.

You will see with horror that most of the texts in this chapter are vulgar copy and paste. Please feel free to send me virtual stones.

In my defense, in case I feel the urge to insure it, I present here patent search sites and each site has its own summarized presentation. I have taken it up each time because I didn't see the point of reinventing the butterfly thread.

Here are some specialized search engines:

For Belgium

https://bpp.economie.fgov.be/fo-eregister-view/search

This tool allows you to consult the complete patents of the Belgian Patent Register, as well as bibliographic data and even the correspondence between the Intellectual Property Office (OPRI) and the patent holders.

It gathers data concerning the scientific or technological description of new processes or technological products or concerning Belgian supplementary protection certificates for medicines and plant protection products. You can also check whether there has been a prior registration of similar or related patents published in Belgium.

The consultation is free of charge and no registration is required (source: economie.fgov.be).

For Switzerland

https://www.swissreg.ch/srclient/faces/jsp/start.jsp

For France

https://www.data.gouv.fr/fr/organizations/institut-national-de-la-propriete-industrielle-inpi/

At European level

https://www.epo.org

Thanks to its worldwide coverage and search functions, **Espacenet** offers free access to information on inventions and technical developments from 1782 to the present day.

Espacenet is accessible to beginners and experts alike and is updated daily. It contains data on over 120 million documents and patents from all over the world. Additional information allows you to determine whether a patent has been granted and whether it is still in force.

You can use Espacenet to:

- Search and find patent publications
- Automatically translate documents and patents
- Track the progress of emerging technologies
- Find solutions to technical problems
- Find out what your competitors are developing.

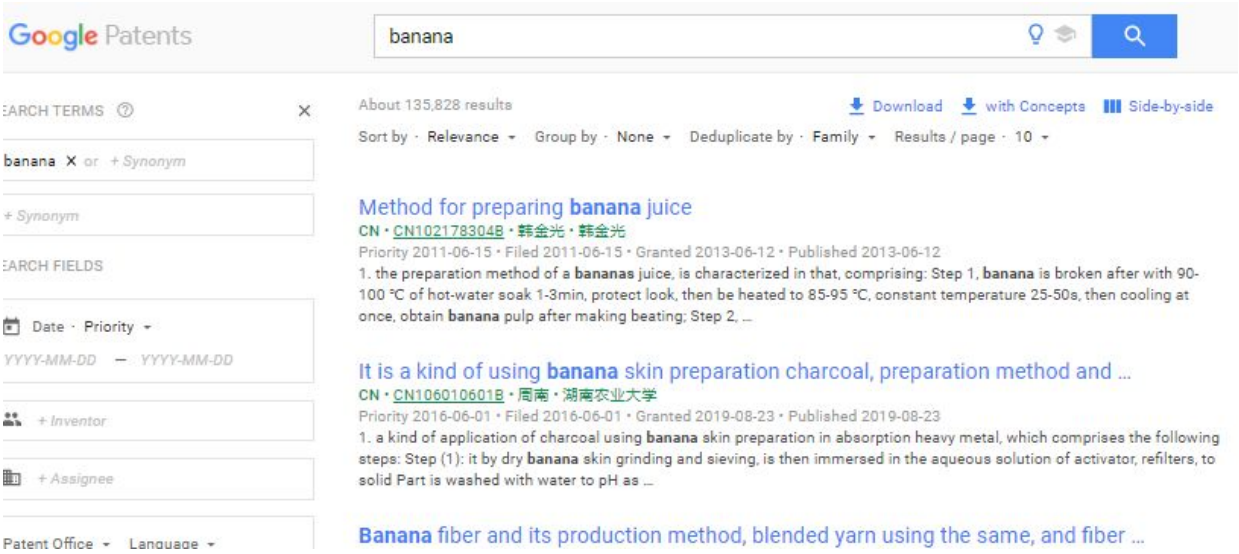
(Source Espacenet)

Worldwide

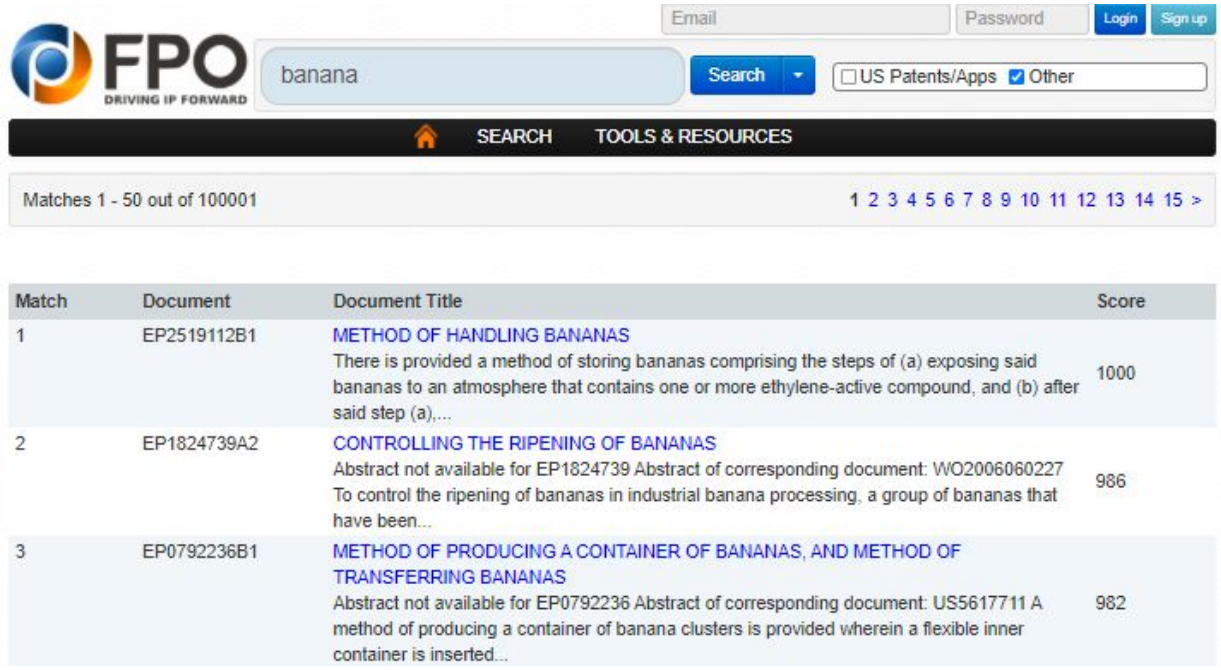
https://patents.google.com/

As is often the case, Google does not like to be outdone. Google Patents is the Google we know, but for the world of patents.

It is not just a simple compilation of worldwide patents; it is a real search engine that works like the Google we use every day. And best of all, the patents are translated into English.



https://www.freepatentsonline.com/ also offers access to all patents, with various easy-to-understand search options. Documents in different alphabets are not translated, except for an introductory summary.



PATENTSCOPE

The **patentscope** database provides access to international applications under the Patent Cooperation Treaty in full text on the day they are filed, as well as to the patent documents of participating national or regional patent offices.

Searches can be made by keywords, applicant names, International Patent Classification categories and many other search criteria in different languages.

https://www.wipo.int/patentscope/en/

Please note that it is also possible to receive alerts, e.g. all new patents of a particular company or the follow-up of a technology.

If you are not interested in patents but in trademark registrations, https://www3.wipo.int/branddb/en/ is a good tool. Simply type in the name of a product or trademark and the site will tell you if it is registered, where, by whom and since when. As a bonus, you get the logo of all the brands that have the word you are looking for in their name.

A search on Chinese patents can be done in English at http://english.cnipa.gov.cn/

11. Tracking changes to a site

Some online tools allow you to keep track of changes to a website. They are particularly useful when you want to track a particular site. Your competitor's, of course but also that of your new partner. Knowing the changes to a business partner's site also means understanding what motivates them to work with you today.

The free version of this tool allows you to track 5 websites. It will tell you what changes have been made to these sites since your last visit. By clicking on the hyperlink of these sites, you will see on the screen the texts that have been modified or added, highlighted in particular colors. You will also have the option of receiving an e-mail alert at the desired frequency, indicating these changes.

A paid subscription is available, which allows you to track more sites.

http://www.trackengine.com

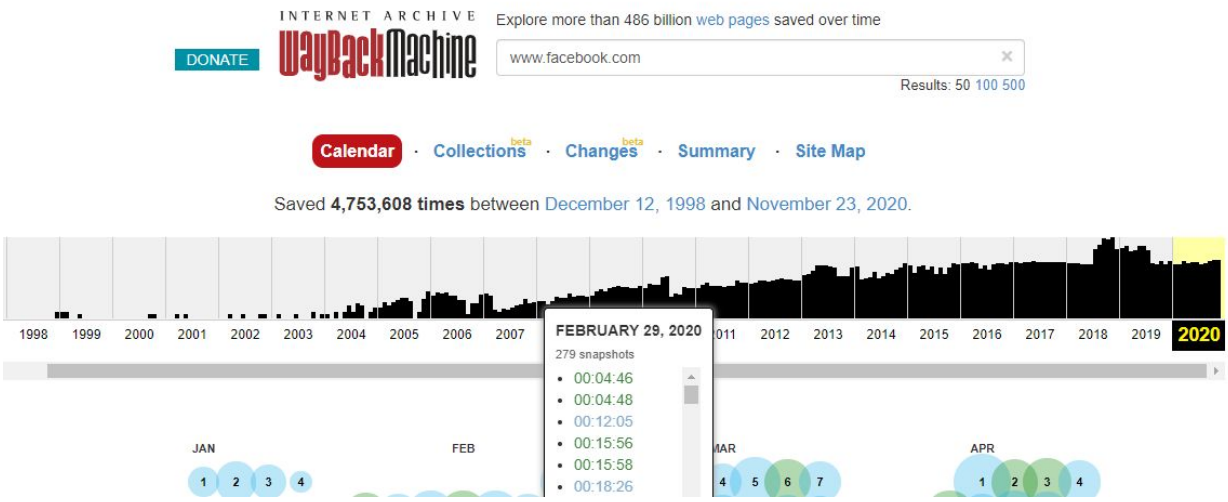
The free monitoring tool by excellence. You can also see price changes of a product or stock changes on a site... Free and not complicated. Here, we monitor the future of a site but it is also interesting to study its past, which allows checking the evolution of a company.

Did you know that the entire web is archived? Indeed there is a site where you can find the history of most websites. Very interesting to see the evolution of your competition or your new distributor.

http://www.archive.org

When you arrive on the site, it looks like a big free library. Don't panic. At the top left of the screen, click on the "web" icon.

Then the search engine "waybackmachine" appears. You type in the url of the company you want to follow, in this case www.facebook.com



The image shows you an evolutionary graph with the date of the first change made to the site, up to the last change made.

Below, you have a calendar with highlighted dates. When you click on it, you get an image of the site on that particular date.

12. Subscribe to your competitor's newsletter

Many companies offer their customers and prospects to subscribe to their newsletter. You can learn a lot of things from it, such as

- How are people who sign up treated?
- How do they respond to emails?
- Is the information they provide valid?
- What do they do that you don't do?
- What's new about them ?
- New collaborators sometimes.
- Collaborations with new partners.
- Pictures of facilities, products, employees.

It's easy, it takes two minutes and it can be interesting. To be on the safe side, you should not send the newsletter to your business address but to a public address such as Hotmail, Yahoo, Gmail (note that some newsletters are only accessible from an email address identified as coming from a company).

As you can imagine, this is not the way to discover an extraordinary secret about your competitor. But often, that's what intelligence is all about. What

you never see at the cinema, otherwise you would leave the cinema, bored to death. We are often in the business of ants, which requires patience and perseverance.

13. Know everything about your competitor's online strategy

Digital marketing is a branch of marketing that I am passionate about. I know that makes me sound like a geek and I'm fine with that. However, this chapter is not about digital marketing. My job here is not to help you promote your products or services but to offer you data collection techniques. We will look at different tools from digital marketing, but with a view to finding information about a target, in this case your competitor.

Spying on competitors' marketing strategies is not as pejorative as it may seem at first sight. It's simply a way of keeping an eye on their digital marketing strateg ies, content, keywords, etc. You do it to understand why they are doing it, why they are outperforming you in certain areas, what makes them tick and in some cases it's even a way to find out what you are doing better than your competitors - to keep improving.

There is a reason why competitive analysis is an important part of developing a marketing strategy. It also provides an excellent opportunity for benchmarking to understand how well your marketing efforts are working.

The truth is that your competitors are probably spying on you too. If you're ranking higher in the search engines, they'll want to know what they can do to change that. If you're more engaged on social media, they'll want to know how to improve their social media strategy to get the same or better results. If your company's blog is making waves in your niche, they will want to improve their own content so they can outperform yours.

Competitor keyword analysis

Keywords are a must if you want to rank well. They boost your visibility, improve traffic to your site and sometimes attract a qualified audience and improve conversion rates.

With **SEMRush** , you can easily search for any domain, keyword or URL and perform a detailed competitive search. You will be able to see what your competitors are doing, what their advertising strategies are, what kind of links they are getting and more. You can also use the data provided to

compare domains against each other. However, if you just want to get your competitors' keywords, insert the URLs of your rivals' sites and you'll be able to see what they are doing.

You will get a list of these with the number of visits each one has managed to generate.

You will also get the results page where your competitor's site appears for the different keywords. You can test SEMRush for free for one week and then it will cost you $99 per month. https://www.semrush.com/

If you want to know your nearest competitor's advertising history and data showing what worked and what didn't work for them, **SPYFU** is a great tool.

By adding this tool to your kit, you will be able to search for any domain and find out all the places the domain appears on Google. As stated on the Spyfu website, you will be able to see "every keyword purchased on AdWords, every organic ranking and every ad variation over a period of time".

Spyfu is particularly useful for keyword research. When you use Spyfu, you simply enter your client's domain and compare it to your competitors.

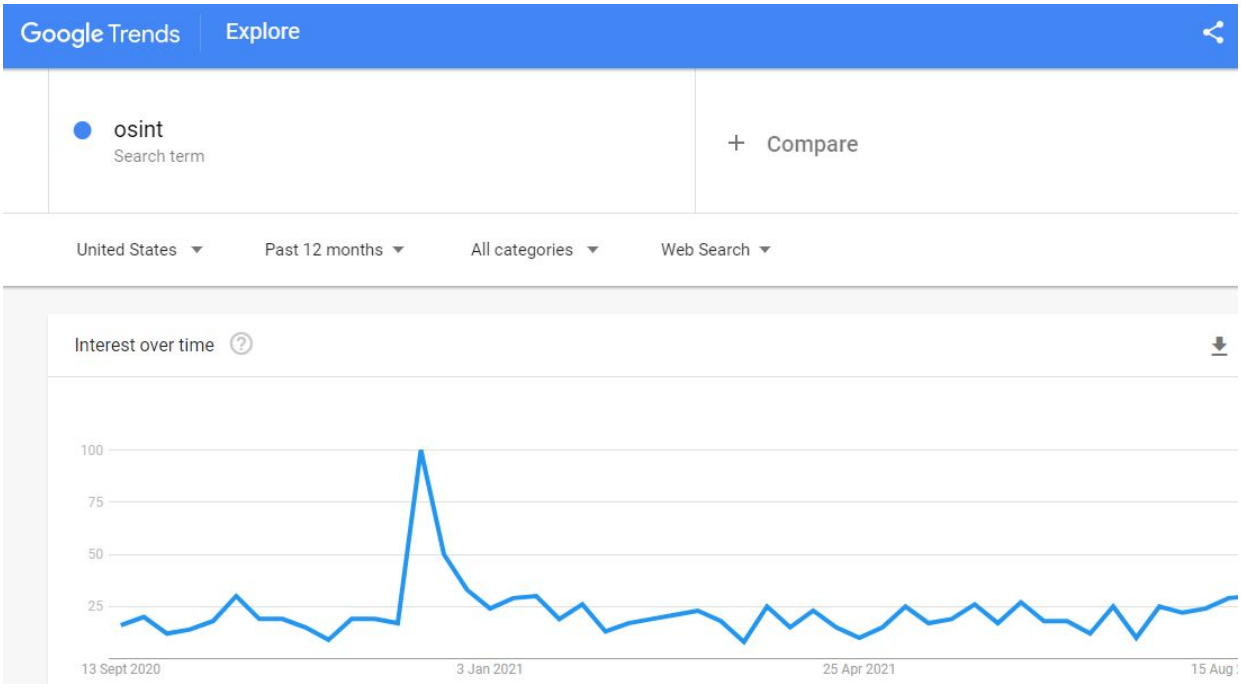
Some features, but there are really a lot:

- AdWords competitor keyword spy tool
- Find competitors' keywords that you don't already buy
- Historical SEO keyword rankings
- Discover and study the overall behaviour of your competitors in terms of their digital marketing

At least, it's quick, easy and intuitive to use. Prepare to be blown away. In short, you will become the best digital marketing spy in the industry.

You can use Spyfu for free, but you won't have access to all the information. If studying the digital marketing of companies is all or part of your business, an investment of $39 per month will not be too much. https://www.spyfu.com/

Google Trends is a free tool for measuring queries. It doesn't just do that, but I use it for that. It allows me to know, over a given period of time, what the frequency of searches on Google is for a given term or expression, the name of your competitor for example.



https://trends.google.com/ is free .

Marketing your competitor on Facebook and Instagram

Facebook itself encourages and allows anyone to view the ads that businesses and organizations run on the site. In March 2019, Facebook launched a tool called Ad Library, designed to promote transparency on the platform. Ad Library allows anyone to search and view all the ads currently running on the site, including Instagram ads.

There are other methods and tools that can be used to evaluate and analyze competitors' Facebook ads, but I have found that the Facebook Ad Library is the easiest and most reliable option available. It is a simple and fairly robust tool that can be used to learn a lot about what your competitors are doing.

Filter by impressions

One of the best features of the ad library is the ability to filter ads by impressions. Facebook defines an impression as the number of times an ad appears on screen for the first time. If you're competing with big names, chances are they're running a lot of different ads. Filtering by impressions is an easy way to determine which ones are shown and seen by the most people.

To filter impressions, start by entering the name of the organization or business you want to view in the search bar and select the Facebook page when it appears. Next, select Filter by Impressions and sort in ascending or descending order. This will display a list of active ads based on the filters you have enabled.

You can also use the Facebook Ads library to see what types of media your competitors are incorporating into their ads. When creating Facebook Ads, you can choose from a number of different formats, including photos, videos, stories, slideshows, etc.

Simply make a list of your main competitors, search for their ads in the library and note the formats or media types they use. Facebook will even tell you if an ad has multiple versions and show you what is different for each of them.

In most cases, different media or messages are tested to determine which performs best when broadcast.

Messages are another good element of ads to pay attention to, especially when evaluating competitors. When looking at your competitors' Facebook ads, you need to pay attention to the headlines they use, the value props they focus on, the points they make and the call to action they use. You want to have a good understanding of how your competitors are positioning themselves and their products, and what promises, if any, they are making to the people they are trying to reach.

Another way to get a better pulse on the best performing competitor ads on Facebook is to filter by duration. When using the ad library, you can filter back up to 90 days to see which ads have lasted the longest. If you see ads that are still active but ran more than 30 days ago, it's probably an indication that those ads were performing well for your competitors.

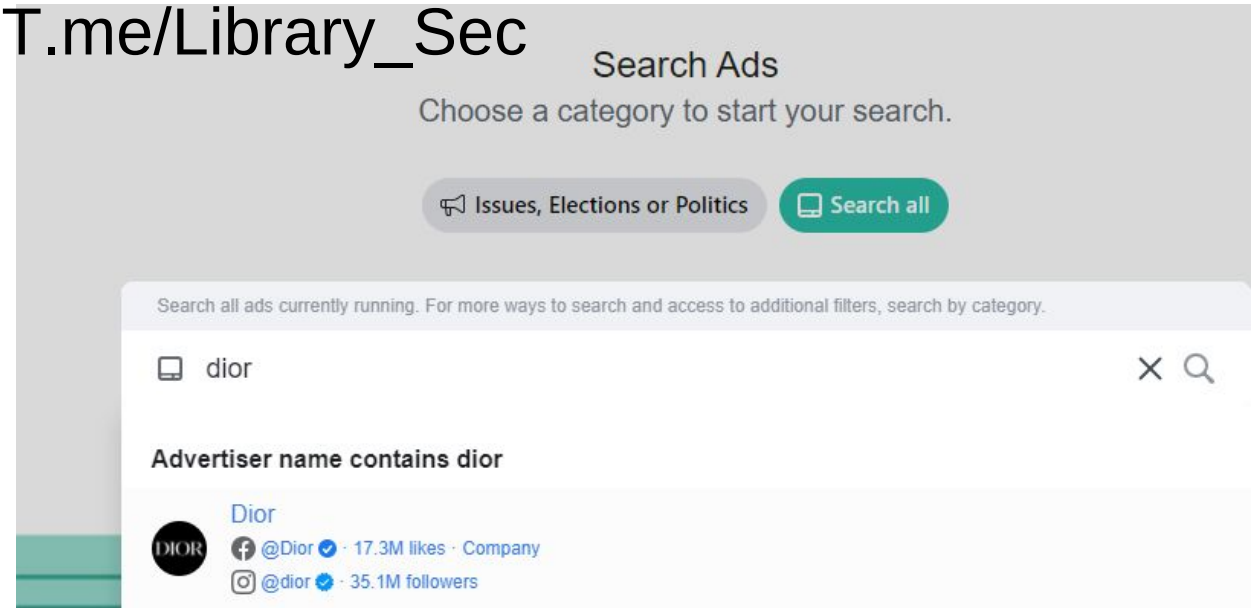
To get a better idea of how long ads have been running, switch from filtering by impressions to filtering by duration. You can filter to see only ads that ran in the last day, 7 days, 30 days or 90 days.

If you see similar trends and ads across several competitors, it is probably worthwhile to run and test a similar ad for your own business.

And you're not stuck with Facebook either. You can use what you've learned to test Snapchat Ads, Pinterest Ads or many other channels. When looking for common themes or repeating trends on multiple pages, pay attention to images, messages, offers and calls to action. You should also pay attention to ads that appear during holidays, seasons or on specific days of the year that matter most to your customers. Then simply apply what you've learned to your own brand to see how it resonates with your audience.

https://www.facebook.com/ads/library

You arrive at a classic search bar. I've decided to take a close look at Dior.



I can sort by country, i.e. look at Dior's online marketing in one country, or in several, or even all. A selection by date is also planned.

I immediately receive the information that Dior has more than 17,000,000. likes and 35,000,000 followers. That's not all, Facebook offers me 200 Dior ads, active or not, in different formats, with the possibility of sorting by date and even by platform: Facebook, Instagram, Messenger.

Another way to get information is to go to your target's page. This time, in order to stay in the luxury category, I chose Porsche and you can take a look at "page transparency".

I click on "see all". At the bottom of the page, I can see if this page is advertising at the moment. I just click and I return to the Facebook bookshop page with the results.

Analyze your competitors' websites

It doesn't matter if you are a computer scientist or not. You MUST study your competitors' site performance. Their weaknesses will be your strengths, and their strengths will be your challenges.

If you want to gather information about your competitor's website, there are hundreds of free and paid tools. **Pingdom** is one of the most popular website monitoring tools. With this tool, you can simply enter a URL and get tons of information about the site's loading speed. In addition to load and response times, it offers specific details and suggestions for action.

Pingdom also offers real user monitoring, which allows you to collect data on site visitor behavior, identify trends and improve the user experience. For example, Pingdom lets you know how a visitor arrives at a site, which is at least as important information as knowing the weaknesses of the site.

Some features are free, you can have a 2 week trial before paying $10 per month. https://tools.pingdom.com/

14. Discussion groups

You follow a blog because you are interested in the point of view of a particular author. Whereas a newsgroup is usually focused on a certain topic, and many different people post their comments and questions on that topic. You follow a newsgroup because you are interested in a specific topic. A

blog is driven by one person, a discussion group by its participants. It is this last point that makes the difference.

Just as there are blog search engines, there are also newsgroup indexes.

These groups (several thousand) are hosted on the worldwide network of newsgroup servers called **Usenet** . Its main purpose is to provide a network where users can freely publish information, which is then broadcast. This allows other people to access information easily and as quickly as possible.

The Usenet is considered to be one of the oldest networks. In fact, it was conceived in 1979. This means that it was set up before the World Wide Web. To access Usenet newsgroups, you need a good Usenet provider.

There are hundreds of thousands of newsgroups on the server and it is possible for any user to create a new one. The Usenet continues to be an unlimited global forum for debate and information exchange.

As new developments continue to shape the internet world and challenge the Usenet as a medium, its popularity continues to grow. People need uncensored, peer-moderated communication in an age where official censorship, or rather social censorship, is taking precedence over freedom of expression.

Focus groups can be an inexpensive way for a small business to learn more about its industry, the competition, and get a sense of new product offerings. This information can also help a company anticipate industry trends and monitor related industries.

Newsgroups are very important in an information search because:

- You receive information from the target customers, often unfiltered.
- You often receive emotional information about the target's perception.
- It is in your best interest to research yourself, so that you know the horrors that people say about you.
- You can practice excessive intoxication, no need to explain how. Newsgroups have invented the global rumor in a click. This is where, thanks to your dedication, the horrified world

will learn that the new ready meal fresh from your competitor has blinded half the residents of a nursing home.

The final advantage is that you will sometimes find messages written by employees of the competition. If you go to the groups and search for the target, you will also see messages left by anyone with an email address related to the box.

The bad news is that there is no such thing as truly free access to Usenet. Well, there is but the nervous breakdowns that are sure to result from using them will cost you more than paying for them. In this book, whenever a tool is free and of good quality, I recommend it and in our business, there are a lot of them but not here, free will means bugs, slowdowns, unwanted ads, and instability.

Let's face it, a lot of people using Usenet do so because there is little or no moderation and they can download porn without risk but it's a great intelligence tool.

Google Groups does basically the same thing as Usenet for free but it has excluded a lot of forums for various reasons, including morality. Which means you can't find everything there. I have given up using Google groups because Google's Usenet archive search function has been interrupted several times in the past, making it difficult to find a particular article.

Downloads on newsgroups are not traceable via the Usenet network. Usenetserver is not free, Count 4 to 8 dollars depending on the promotions.

https://www.usenetserver.com/
https://groups.google.com/

15. Blogs

A blog differs from a newsgroup in that it is run by one person, often on a particular topic. Following your competitor's blog closely is an essential part of your competitive intelligence.

The idea here is to get an idea of how effective your competitors are at blogging so that you can start to develop a strategy that builds on their successes and exploits their weaknesses. Here are some things you'll want to look at:

What types of blog content do your competitors publish? Tutorials, information about specific products, videos, homegrown articles or links?

Are there any obvious gaps in your competitors' existing content? Quality, originality, freshness of information, spelling etc.

Many bloggers use a personal writing style that the reader recognizes immediately. Or, depending on the subject of your blog, perhaps a more formal, almost academic approach works better. Either way, check how your competitors deal with this issue.

When do they ask readers for comments or suggestions, and how do they formulate these requests? Do readers actually respond, and to what types of approaches?

How often does the blogger post new articles on the blog: the frequency of blog posts is an important question. All bloggers will tell you to post "frequently", without really defining what that means.

Posts that get a lot of comments and those that get very few: A blog that gets a lot of comments is a sign that the blogger is resonating with their audience. A blog that receives few or no comments probably leaves people indifferent and may simply not be read.

Some posts are better received than others, and part of a blogger's success is knowing what makes those posts really work, so they can repeat them. Monitor your competitors' blogs to see when an article gets a significant response, and see what that response is.

Official company blogs are less interesting than those made by employees or customers of the target. As in newsgroups, you will find qualitative, emotional, and sometimes sensitive information: an employee disgusted with his employer, the opinion of a frustrated or super satisfied customer. Basically, the same kind of informati on you will find in newsgroups.

If your target is a famous stranger, there is no need to bother: a simple Google search will give you direct access to the information on the blogs. If Google gives you thousands of references, then it is interesting, as with newsgroups, to carry out a specific search via a search engine focused on blogs.

https://www.blogsearchengine.org/ is a blog search engine that uses Google's technology.

16. Newspaper and magazine archives

Newspaper and magazine archives are full of good information about businesses and entrepreneurs. Some are free to access, others are not.

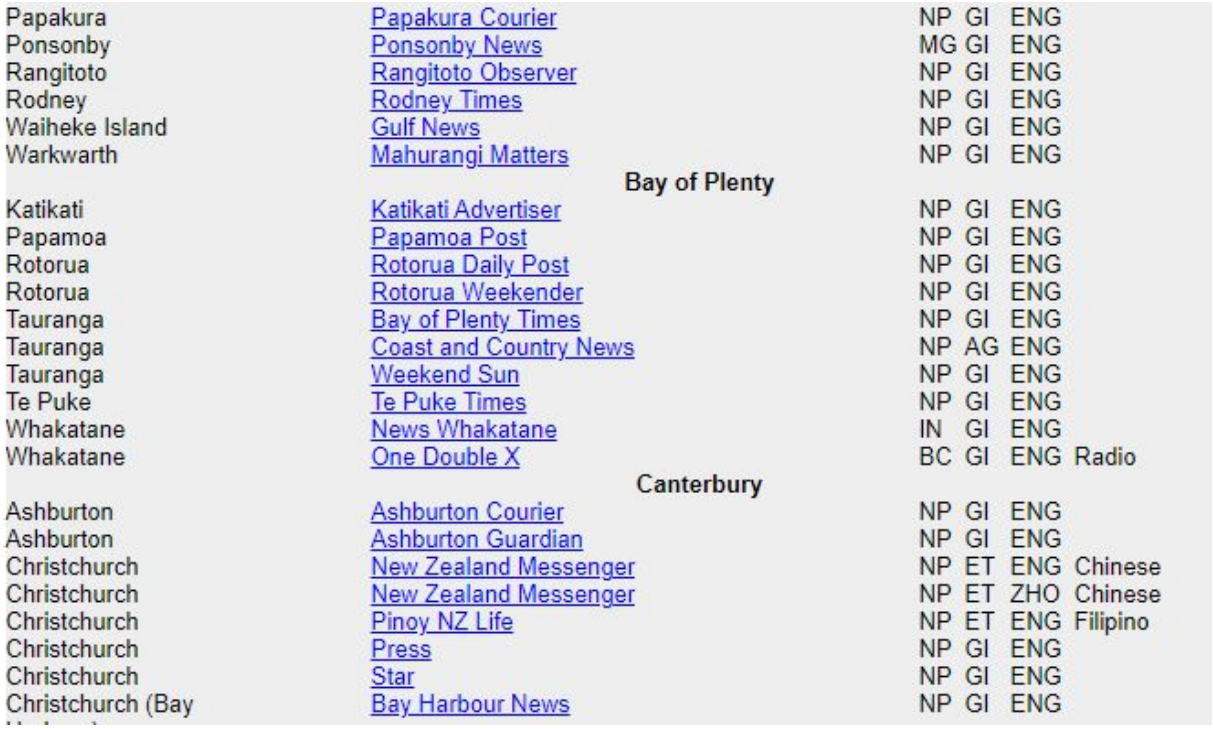
There is no need to go to a media site to do your research. Google and Boolean science have come a long way. On this subject, I strongly recommend that you read the first chapter of this book in depth.

In the example below, I am looking for articles in Liberation, talking about private detectives, and so I type site:www.theguardian.com which will give me results only from this newspaper. I associate it with "private detective" and Google only shows me articles on this subject in the newspaper "The Guardian". By clicking on "tools" at the top right of the page, I will be able to refine my search according to the periods I want.

I would like to point out that I used this method when investigating the possible future partner of a client, and I found a superb photo of the gentleman in question, handcuffed between two carabinieri. I would have found the photo anyway by doing a classic Google search as it was archived in Google Images.

If you are investigating in a country other than your own, you probably don't know the local newspapers or other media. However, this is a major source when investigating a person or a company. http://www.abyznewslinks.com/

is an extraordinary index of the world's media. Not only does it give references to the main national media, but you also have references by state and even by city.



Papakura	Papakura Courier	NP	GI	ENG	
Ponsonby	Ponsonby News	MG	GI	ENG	
Rangitoto	Rangitoto Observer	NP	GI	ENG	
Rodney	Rodney Times	NP	GI	ENG	
Waiheke Island	Gulf News	NP	GI	ENG	
Warkwarth	Mahurangi Matters	NP	GI	ENG	
	Bay of Plenty				
Katikati	Katikati Advertiser	NP	GI	ENG	
Papamoa	Papamoa Post	NP	GI	ENG	
Rotorua	Rotorua Daily Post	NP	GI	ENG	
Rotorua	Rotorua Weekender	NP	GI	ENG	
Tauranga	Bay of Plenty Times	NP	GI	ENG	
Tauranga	Coast and Country News	NP	AG	ENG	
Tauranga	Weekend Sun	NP	GI	ENG	
Te Puke	Te Puke Times	NP	GI	ENG	
Whakatane	News Whakatane	IN	GI	ENG	
Whakatane	One Double X	BC	GI	ENG	Radio
	Canterbury				
Ashburton	Ashburton Courier	NP	GI	ENG	
Ashburton	Ashburton Guardian	NP	GI	ENG	
Christchurch	New Zealand Messenger	NP	ET	ENG	Chinese
Christchurch	New Zealand Messenger	NP	ET	ZHO	Chinese
Christchurch	Pinoy NZ Life	NP	ET	ENG	Filipino
Christchurch	Press	NP	GI	ENG	
Christchurch	Star	NP	GI	ENG	
Christchurch (Bay	Bay Harbour News	NP	GI	ENG	

The table above is an example from New Zealand. The site provides a breakdown by country, region and city, as well as by media type, speciality and language spoken.

If your target audience is active in any media or social network, https://yougotthenews.com/ will find it. Whether it's a newspaper, a blog, an article in Linkedin or Facebook or even a simple comment to an article. The Yougotthenews engine uses Google, but does a better job than if you go directly to Google. How does it do this? By using advanced Boolean formulas in its queries. The site doesn't have an extraordinary design and this is to better hide its power.

Definitely a key tool for the investigator.

17. Identify the competitor's customers

You want to identify your competitor's customers either because you know you are so strong that you will poach them o r because they will be a fantastic source of information for you.

"I notice you use technology X, do you have 15 minutes to try and compare our software?"

In a free market economy, it is common for B2B companies to poach their competitors' customers.

Part of the B2B sales strategy is to find out who uses or compliments your competitor's products and services. In a cold call approach to prospecting, you can admit that you already have a point by starting the conversation with "I know you use technology X". Normally, you will attract attention.

Another advantage of finding out who the competitor's customers are is that you save time. In traditional cold calling, you don't know if the person you are calling needs or wants what you are selling. In fact, most of the time, the answer is "no thanks" but if you have a list of the competition's customers, the question no longer arises. You know that the customer is a user of what you are selling and you also know that they can afford it. The ultimate bonus is that since you know who the prospect is buying from, you know how to make a very powerful argument in your favor and if you don't have one, change companies.

There are many methods of identifying the competitor's customers. They can be simple or complex, legal or not. You probably won't be able to use them all.

Check the competitor's website. Often you will find customer references, but I don't really like references because you will only get the super happy customers.

Pretend to be a potential client and ask for references. This is good, but the same problem as in the previous point. You will only get happy customers.

Take a look at Internet forums and type in the name of your competitor. Not only are you likely to find names of customers, but you will also get their comments.

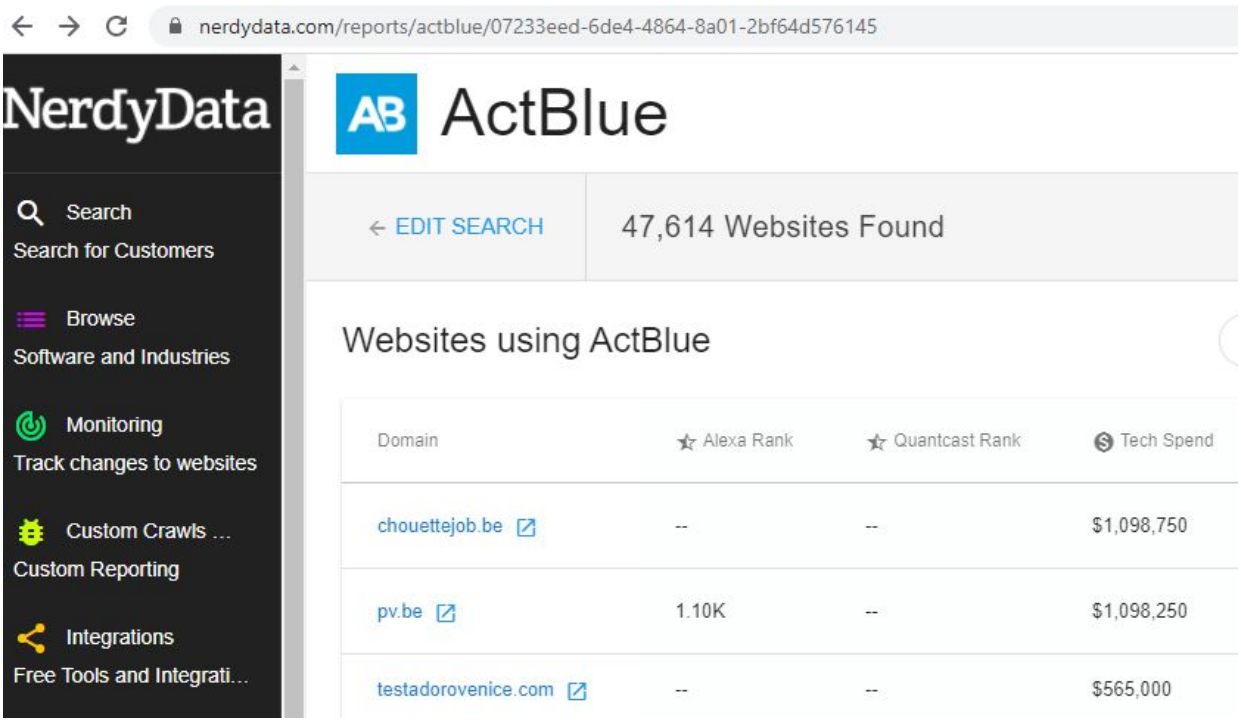
Do a Google search, you type in the name of the competitor or the name of some of their products if they are a manufacturer, you may be able to find the names of some customers.

You have an informant who works for tax administration and this nice person will give you the VAT listing of your competitor.

Source code search engines allow you to find all companies that use a particular technology, including your competitors. How does it work? The engine scours the web for codes placed on websites. Codes can be CRMs, shopping carts, hosting, tracking, analytics, scripts, plugins, etc.

For example, if you sell an online payment platform, you can find all websites that use a competing product.

https://www.nerdydata.com/



Here I learn from Nerdydata that 47,614 sites use ActBlue's technology for their payments.

If you market a technology related to the net, this site is a good one. Not only can you identify who is using what, but you can also find out who changed technology and when.

LinkedIn Sales Navigator allows you to filter out companies that use a particular technology. It could be a competitor or a complementary product.

You are patient or you have big money and shadow your competitor's sales people or delivery trucks. Of course, this technique is mostly applicable in your country, although no one is stopping you from hiring someone to carry out the mission abroad. Pay attention to one detail that may be important, this is all legal. As long as you are following someone on the street, no one can tell you anything, unless the person in question files a complaint for harassment, which is unrealistic.

Of course, if for reasons of economy and efficiency, you have stuck trackers on your competitor's vehicles, this is no longer legal at all.

There is another method, possibly complementary to the previous ones. It costs a bit of money, but when you think about it, it will be cheaper than

tailing the salesmen or the delivery trucks. Use students; Let me explain. Your competitor must have a target. Define the target. Here I'll use an example, it will be easier to understand.

Let's imagine that you sell used oil. The customer base is made up of garages and car dealerships. You draw up a list corresponding to the target clientele and your students call them all under the pretext of a notoriety study. To keep it cheap and quick, ask a minimum of questions. It's something like this. "Hi, I'm Jerome, I work in a market research company and I'm carrying out an awareness survey. I would like to know, in the following list (the student reads a short list of brands of used oil, obviously including your competitor's brand and yours) which brands you know. Second and last question, can you tell me which of the brands you know are the ones you use in your work?

You use a student for two reasons: the first is that it is cheap. The second is that the call completion rate is higher. People often answer the phone that they don't have time to answer these questions but when you have a young person on the other end of the phone meowing “Pleeeease it's to pay for my studies, it'll take two minutes", it's immediately more complicated to hang up. I did it a lot when I was a student and very few people didn't answer the questionnaire.

Finally, the greatest advantage of the method is that you kill two birds with one stone. Not only do you identify your main competitor's customers, but you will certainly make the operation profitable when the student brings you some hot prospects who are not at all satisfied with your competitor's services.

It's simple, it's fast, and you'll have created complete lists of competitors' customers in a day or two and what is valid for oil change is valid for just about anything. With such a small questionnaire, an operator will call between 50 and 100 companies a day. It won't be long before you have a complete list of all your competitor's customers, or close to it.

On Facebook or LinkedIn, you can find out who likes a post or a company page. You can also join a dedicated group and identify many users. What is a bit complicated here is that you will have to sort out the people who are close to the competitor's product or service (family, friends, employees etc), and those who are users.

18. Identify competitor's suppliers

Do you think that one of your competitor's suppliers makes a difference? Here are some tools to help you identify your competitor's supplier(s).

- When you type in your competitor's name on GOOGLE, you may be surprised to find that your competitor is listed in the customer reference list of a supplier.
- It can work as a bluff, by pretending to be a potential customer, you demand to know the origin of certain components of the product you are buying, under the pretext that everything must be organic, iso thingy or made in North-East Europe or whatever. A sales manager won't give you the information, but a salesman might.
- You can go undercover at the exit of your competitor's company and take pictures of all the trucks that come into the car park. This way you have a good chance of finding various suppliers. Of course, anything delivered by independent transport companies will be missed.
- If you are looking for a particular supplier, you will probably have to make contact. When I say "go to contact", I am not talking about intrusion. Neither physical (burglary) nor IT (hacking). To me, intrusion is a dumb thing to do. Even if you are an ex-CIA agent, breaking into a company's offices at night to plunder its secrets is a huge risk. Since you won't be doing it yourself, you'll have to hire someone for the job.

And if that someone gets caught, do you think the mobster's code of honor will work for you? or will they give you up in exchange for a benefit? Again, the distinction between film and reality is relevant. In reality, the offender talks unless he fears for his own skin or that of his family. Since you are just a poor executive without biceps, he will not fear you. If he doesn't rip you off, that's a miracle. If he is caught, you will be caught.

It's the same with computer intrusion. Today, the crime is so costly (several years in prison) that few people are willing to take the risk. Those with hacking skills are easier to find than burglary specialists (any computer security consultant is a potential hacker), but they will also be much more

reluctant to commit a serious crime that could send them to prison for a long time. In general, the cops at the CCU (Computer Crime Unit) are no fools.

You can easily find proposals for hackers on the net. Most of them come from Eastern Europe, but you will also find some from North Africa. They will ask you for a small advance payment via Western Union and the job will never be done. If the job is done (it happens) you take a crazy risk: the hacker knows you and he can blackmail you which he will. As you will have understood, these are not ethical considerations which, in my view, exclude intrusion into the world of economic intelligence. The risk is too great. It leaves traces.

So, I come back to "going to the contact". The best people to give you the information about a supplier are the employees of the competitor. If you are looking for a particular supplier, you can get the info:

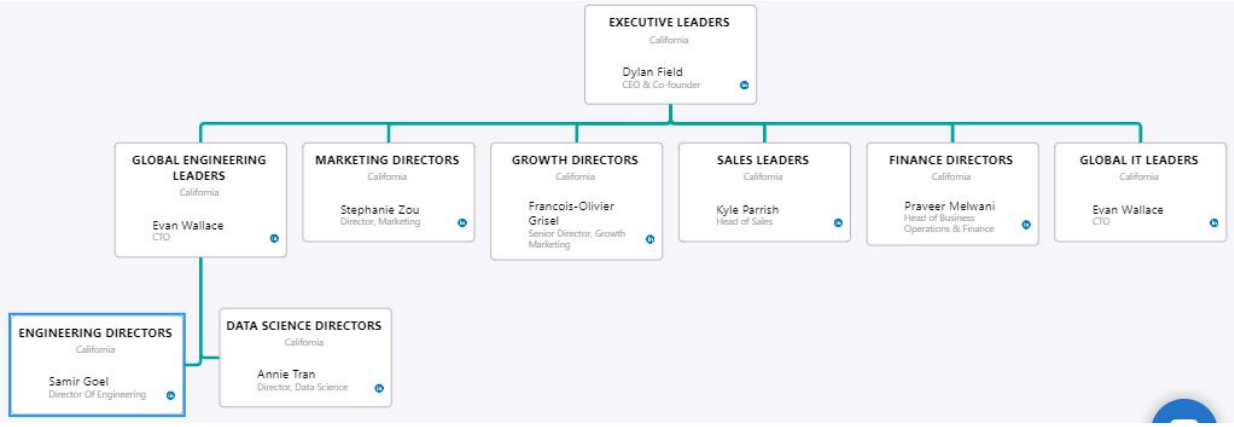
- By posing as a potential supplier of that type of material to your competitor. You try to meet your competitor's buyer and get him to talk.
- By posing as a customer.
- Inviting a key executive to a "screening interview".
- Pretending to be a journalist.
- Visiting the client's premises (pretending to be a salesperson of any kind).
- At a trade show, pretending to be a client.
- By using the same "market research" technique seen in the paragraph on "how to identify the competitor's customers", i.e. by phoning the buyer under the pretext of a study on a product range, quoting brands, asking if they know them, and carelessly asking them at the end what brand they work with. Obviously, do not insist if they do not want to answer.
- Your competitor's employees are going to lunch. Prepare a good catchphrase to start a conversation. An interesting target in this case will be the stock manager. You can of course meet him or try the market research technique on them.
- Use photos of products sold by your competitor by running them through the various reverse photo search engines. You have a good chance of finding the origin.

19. Your competitor's organization chart in one click

Identifying your competitor's employees is relatively easy. Structuring the information into a company organization chart is much less easy.

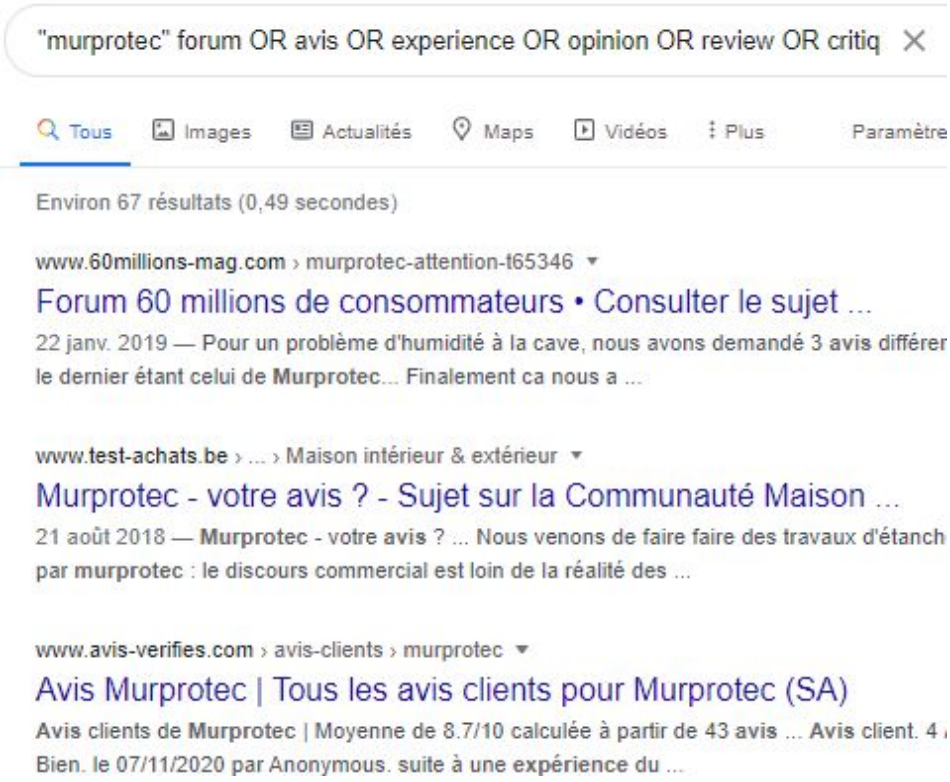
Chartloop is the first intelligent organizational charting platform that allows you to automatically visualize the organizational structure of any company. Most people use Chartloop to map their target sales accounts, to build better recruitment pipelines or simply to get strategic information about competitors.

www.chartloop .com



20. The reputation of your competitor

What customers say about your competitor is an important asset. You know the perceived strengths and weaknesses of the company. Once again, Boolean methods fit the bill perfectly.

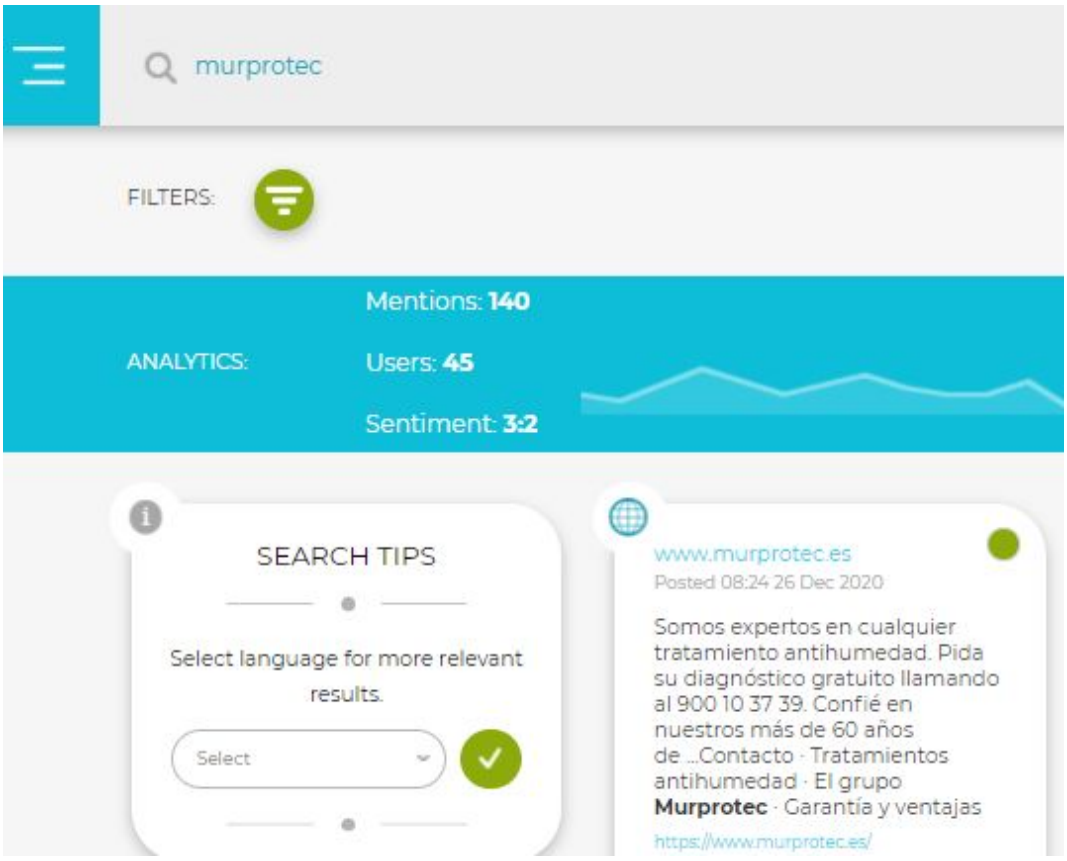


Here, I do a search on Murprotect, a Belgian SME providing services to individuals. I type the name of the company followed by various words in inverted commas: forum, opinion, experience, review, critique etc including "OR" between the company name and each word. If your target is international or English-speaking, the company name followed by the word "review" will be sufficient.

If you don't want to bother, "**Social searcher** " does an excellent job. It is not the only one, there are many.

It allows you to monitor all public social mentions in social networks and on the web. You can measure and track what people are saying about your competitor, their brand, their products etc, in an easy to use and understand dashboard. There is also an alert system that warns you when a new comment is posted on a network.

It is a free tool within a certain limit and is quite large but for 3.5 euros a month, you have access to everything and it's impressive because you can search for social networks with keywords or expressions, and also search for information on people or trends, through seven social networks. This increases to eleven networks when searching for a brand or a company.



The slightest whisper from Twitter or Instagram is just a click away.

Social searcher also offers you search filters whether it's language, expression of positive or negative feelings, social network, date etc.

https://www.social-searcher.com/

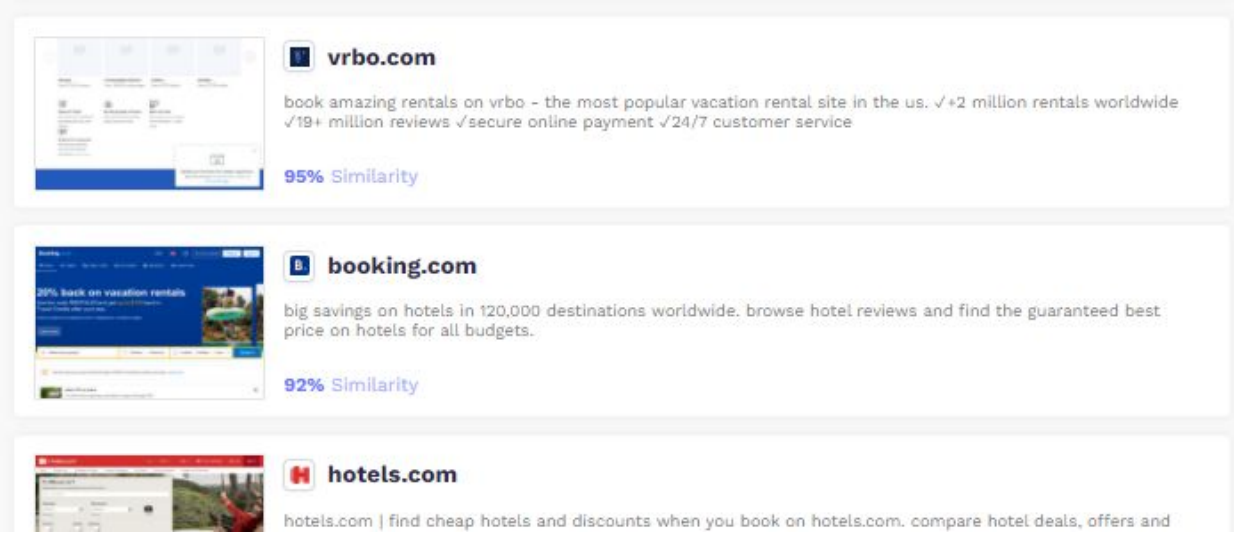
I guess there's no point in suggesting that you start searching for yourself with this wonderful tool, which will take about 8 seconds of intense concentration to get the hang of.

In addition to finding out about your competitor's reputation, it is interesting to know their world.

Here are two ways to do this;

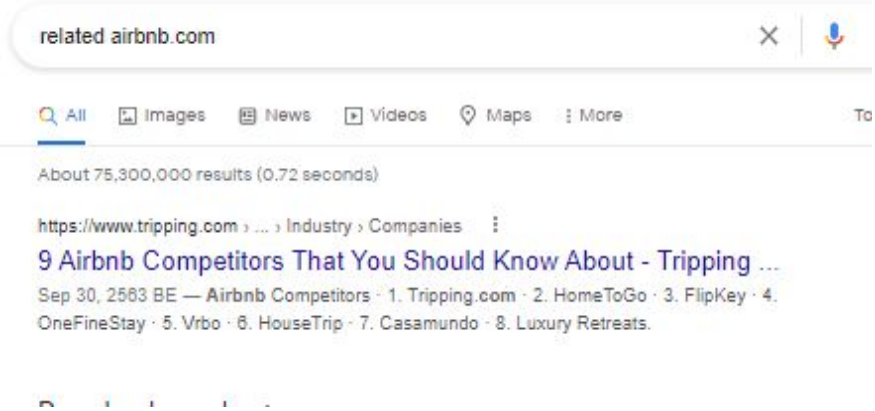
Firstly, you have specific sites such as **similarsites.com** , which allows you to find sites similar to the site whose address you have entered. This is a good way to get a feel for the world your competitor is in, provided it is a site with a significant number of visits each month.

If I do a search on airbnb.com, this is what I get:



https://www.similarsites.com

Another way to get a similar result is to use a Boolean trick, namely the word "related" typed into google.



If you need to research a company's environment, I suggest you use both tools. Again, your target must be of a certain level, otherwise Google will not bring back anything interesting.

21. Finding value-added information via databases

Sometimes we have a slight tendency to forget to keep things simple. Not long ago, a client asked me where he could find a database of electricians. When I replied "well, in the Yellow Pages", I could see that he was feeling a

little silly but he just had a reflex that many of us have and I could have had the same one: look for complicated when you can do simple.

Public databases are a mine of information. But, before starting, let me give it a thought first: many of these databases provide a wealth of information, free of charge or at very accessible prices. One very important thing to remember is that this information is about the past. Sometimes the recent past, but always the past. Getting the balance sheet of your competitor or a future partner is very useful, but don't neglect to investigate what has happened in that company since the balance sheet was published. We shall come back to this later.

A) Accessing European business registers

Through the following link, you can access all registers of the European Union countries (plus Norway, Iceland and Liechtenstein). For each country, you have a description of the information available in the country.

If the link below is too complicated to type in, go to Google and type in "business directory in member states". This little page is nothing less than a great source of business information.

https://e-justice.europa.eu/content_business_registers_in_member_states-106-fr.do

There is a search engine that works across 20 European countries, the European Business Register. It works through various companies and you have to pay to access it, whereas if you go to the above address, it is free.

This paid engine has one advantage, however, which is that it allows you to trace a manager's name in all member countries. But not all countries are present in this engine. For example, Belgium is not included.

https://www.ebr.lv/en/company-search

B) Directories from around the world.

https://www.searchenginesoftheworld.com/ is a site that centralizes all the directories in the world, whether they are personal directories or directories of businesses and companies. The world of directories is constantly

changing. There are therefore quite a few dead links but this site remains a must in the virtual library of the investigator.

C) Going further...

Opencorporates is a worldwide database of companies. Access is totally free. I might as well say that, it's a great tool for an investigator because you can see the representation of a company worldwide with one click.

When I do a search on EDF, the site finds 1435 companies worldwide. Probably not all of them are related to a certain French energy supplier. It's

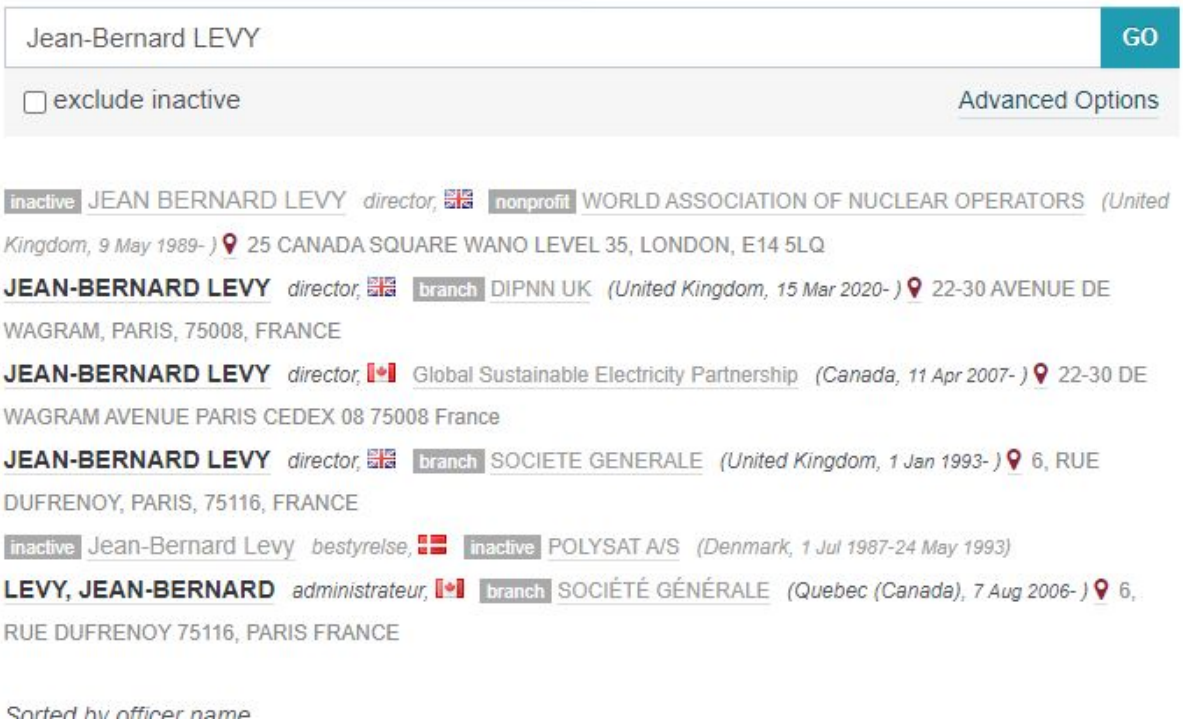
up to you to sort it out. You will be helped by the advanced options.

For an investigator, inactive companies are often at least as interesting to investigate as active ones. Opencorporates allows you to do a wide variety of sorting.

For each company, in each country, the site provides a link to the local trade register where you will find, among other things, the company's founding documents.

As you can sort by country, you may learn that a company has operations in unexpected countries. You can also find patents filed by a company or one of its subsidiaries around the world.

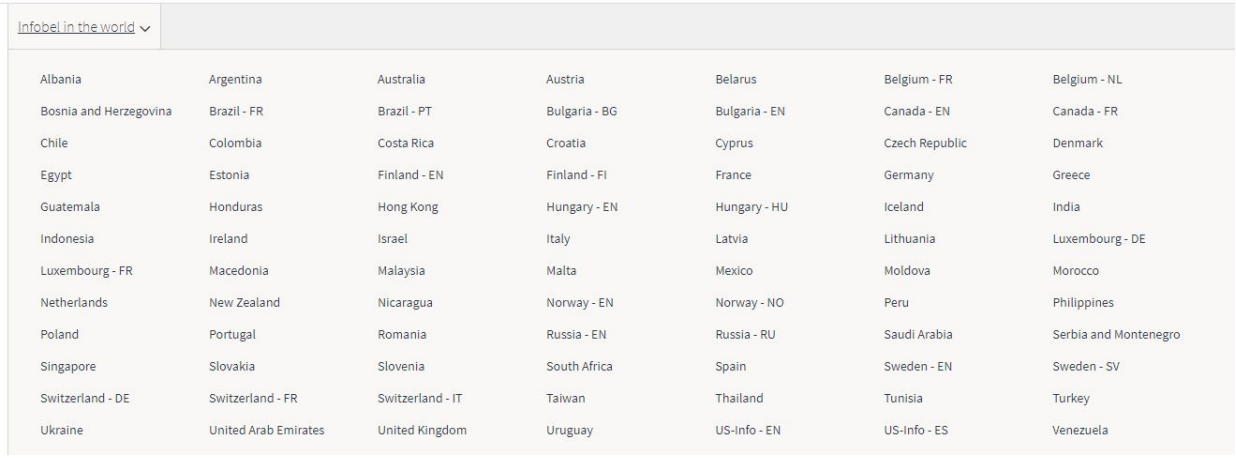
An interesting form of sorting is the possibility to find out the status of a company and what type of company it is. I can also search by company directors. Since I am on EDF, I might as well continue with Jean-Bernard Levy, its chairman.



You might think that the site is only interesting for big executives and big companies, not at all. You won't find anything about the corner shop, but if you're looking for information about an SME, you'll certainly find it.

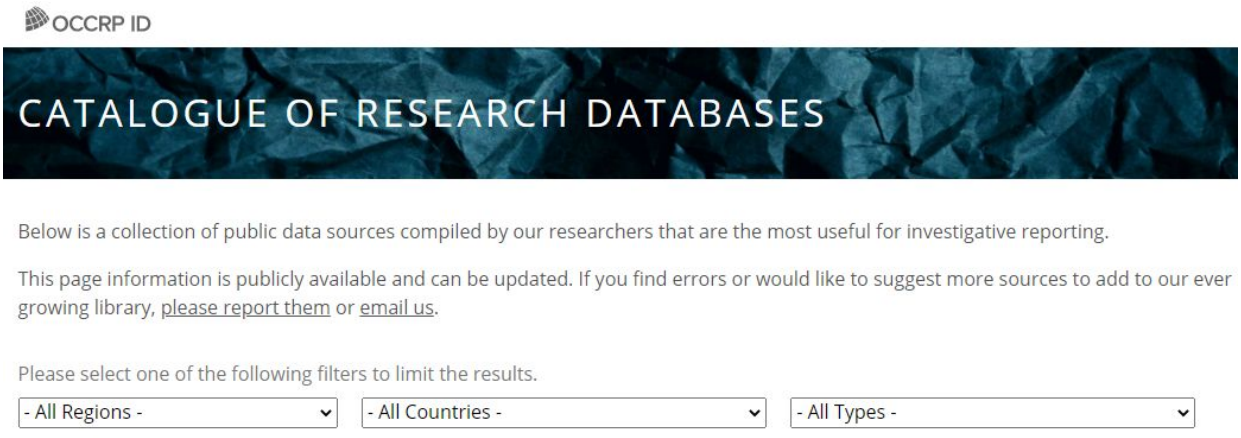
https://opencorporates.com/

Infobel is an international business directory. It is the equivalent of the yellow pages for 94 countries. A single site gives you access to information on millions of companies worldwide, with some financial data in each case. A simple, free and Belgian tool.



https://www.infobel.com/

The Organized Crime and Corruption Reporting Project (OCCRP) will help you trace people, companies and assets around the world. It is an international network of independent media and journalists. You have access to almost 1000 public information sites on companies around the world.



https://id.occrp.org/databases/

The **Aleph Project** is part of the OCCRP where you will find millions of documents from all over the world about past or ongoing investigations of

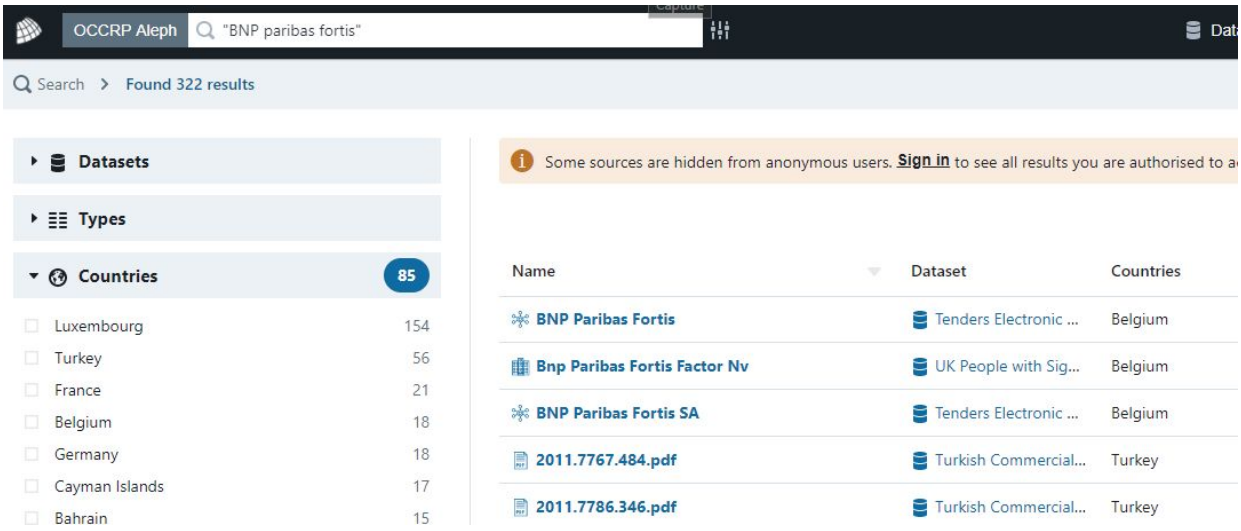
individuals or companies.

The Aleph data platform brings together a vast archive of current and historical databases, documents, leaks and investigations.

While the purpose of this site is journalistic in nature, to expose fraud and corruption, it will also be useful for any investigator looking for sensitive information. Note that the focus here is on the big guys.

You won't find much about the electrician who took your deposit before disappearing into thin air.

But if you do a search on a group like BNP Paribas Fortis, you will come across hundreds of documents related to investigations, in a large number of countries.



https://aleph.occrp.org/

The **ICJ database** contains information on more than 785,000 offshore entities that are the subject of the Panama Papers investigations, and other financial scandals. The data links to individuals and companies in over 200 countries and territories. The interest here for an investigator is in verification. You're considering a partnership with a person or company and you look here and hope it's not there.

https://offshoreleaks.icij.org/ does a complementary job to the previous one. These sites are indispensable when you are investigating a company or simply because you have a compliance-related mission.

https://www.anti-moneylaundering.org/ The **AMLLIG** has developed a website to assist lawyers in complying with client identification/verification and suspicious transaction reporting requirements in light of the EU Money Laundering Directive in Europe, as well as other money laundering regulations.

The **IBA Anti-Money Laundering** Website is the first one-stop-shop for access to the most current versions of new anti-money laundering laws and regulations that have a significant impact on the legal profession. The website currently features coverage of lawyer's responsibilities in connection with anti-money laundering legislation in over 100 jurisdictions.

You don't want to work with a company or person who is on a list of fraudsters or in connection with terrorist financing. Unfortunately, these lists are scattered around the world and if you want to search them, it will cost you. **Altares** is the world's leading provider of corporate information, in partnership with Dun & Bradstreet. You will also find almost all the credit information you need.

https://www.altares.com/fr/

It has two competitors:

The Van Dijk office https://www.bvdinfo.com/en-gb/ and Ellisphere https://www.ellisphere.com/?lang=en

Biznar is a deep web search engine that returns high quality results by submitting your query to other search engines and collating, ranking and dropping duplicates in the results. The engine will search for information in a series of sites dedicated to business in the broadest sense. Its strength is that you can find information even on small companies. https://biznar.com/

Xlek is a unique database. It gives you all the information you need to know about a person living in the United States: the search for people, property records (including appraised value of property), vehicle records, court records (convictions are public in the US), patents, business registration, domain name registration and even access to the White House visitation log.

Many sites offer this kind of service. What makes Xlek special is that access is completely free and reliable. Two qualities you will rarely find in the US. Reliable databases have to be paid for, which is not a problem because the

rates are very affordable. The problem is that if you are not in the US, you won't have access to most of them. A VPN won't save you because your credit card will be kindly declined. https://xlek.com/

There are also databases with the names of people suspected of financing terrorism or more generally, that banks cannot take as customers. I shall talk about this later, in the chapter on your business partners.

VIII. The best tools and techniques for extracting emails

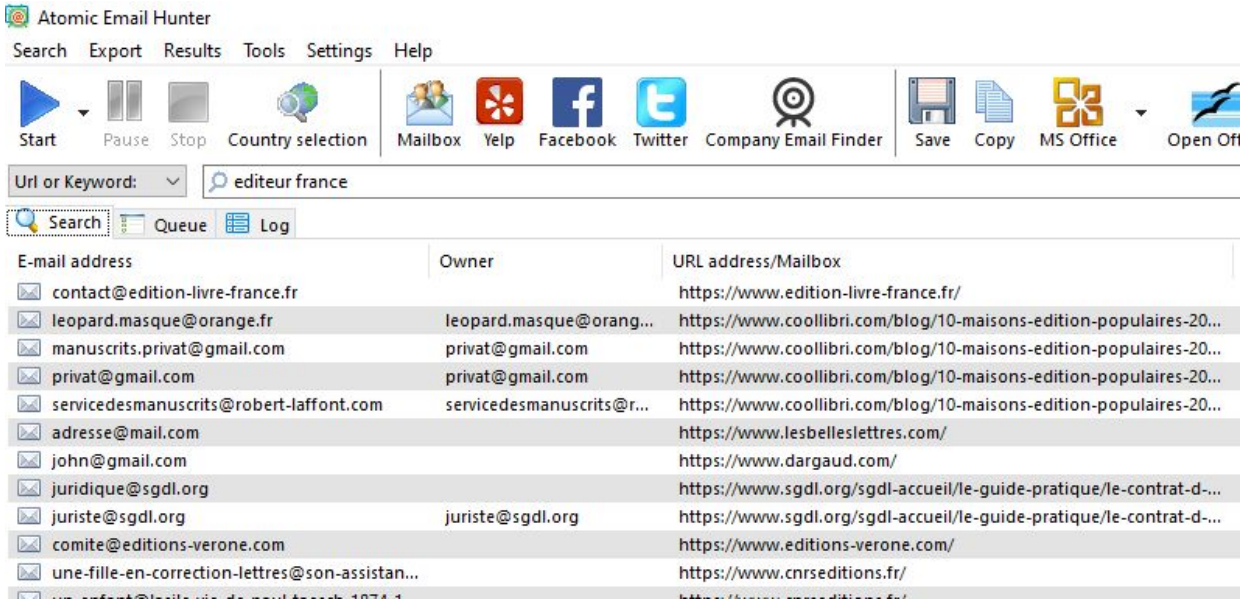
You've been told that emailing doesn't work anymore, that it's outdated, cheap, bad, and illegal without the consent of the person receiving your message, that you'll be fined or even sentenced to death. Nonsense. As long as you are careful and reasonable, which mainly means not harassing people. My rule has always been simple: each person in one of my databases can receive one or two mails per year. No more than that. I have been doing this for more than ten years and the worst thing that has happened to me is a letter from a government department telling me that someone had complained and that I was asked to send them a letter confirming that I would never use that email address again. In the interest of privacy, the ministry in question gave me the person's private address so that I could send him the letter, which I did.

I started email scraping as soon as I wrote my first book. My first concern was to find a publisher. I didn't know any except for the ones I saw in bookshops. I was neither known nor introduced in the right circles and I knew that only one book in a hundred is published. Nor was it conceivable that I would print the book in dozens of copies and put them one by one in an envelope before sending them by post in the hope of being spotted by a reading committee.

So I decided to use email scraping techniques. Initially my plan was not to be published, but to do everything myself, including promoting the book via journalists. I created a database of journalists and used it to promote myself. Later, when I got tired of doing the job of a publisher, I created a database of French-speaking publishers and sent thousands of emails with the table of contents. As I love a good story and so do you, you should know that about twenty publishers have asked me to send a copy of the book, that six have made me a firm proposal and that I have signed with an important French publisher.

Atomic Email Hunter was the first tool I used. It's a robot that goes around the net and extracts emails in two different ways:

- You have identified, thanks to Google, directories containing the contact details of publishers or journalists and you copy/paste the url of the site into Atomic and off you go. If the site is not too protected, all the emails will be swallowed by your little robot.
- You use the Atomic engine with search criteria by country or region. It's not terribly precise but it works. You will still have to sort manually to remove addresses that do not match your search.



Then I can extract the resulting data and open it in an Excel file.

Atomic does not work with PDF files. If you have a link to such a file, you can still get it to work. You open the cached file by clicking on the little inverted triangle and then on "cached".

Finally, you copy the address into the Atomic search bar and run it. The address will always start with "googlecache".

You can try it for free but you will not be able to export the data. You can therefore test the efficiency of the software, but not enjoy the results. Budget 90 dollars

https://www.atompark.com

A second tool that I like is **Annucapt.** Annucapt allows you to retrieve data from the main directories in France, Belgium, Switzerland, Luxembourg, Germany, Italy, USA, Great Britain, Canada, Spain, Monaco, Morocco and access to the worldwide directories of Yelp and Infobel. The information is provided in a structured way, like an Excel file (which you can export to) with the company name, address, phone, email, web etc.

As the directories sell their data, it is a permanent war between them and Annucapt. Very often, the extraction of a directory does not work anymore or only partially. Annucapt very quickly proposes an update that fixes the problem, until the directory has again found a solution.

Overall it works very well. Annucapt is a classic web retrieval tool, but that's not why you buy it.

Budget 125 euros with the possibility to try it but you won't have access to all the features nor export the data.

https://www.atompark.com/

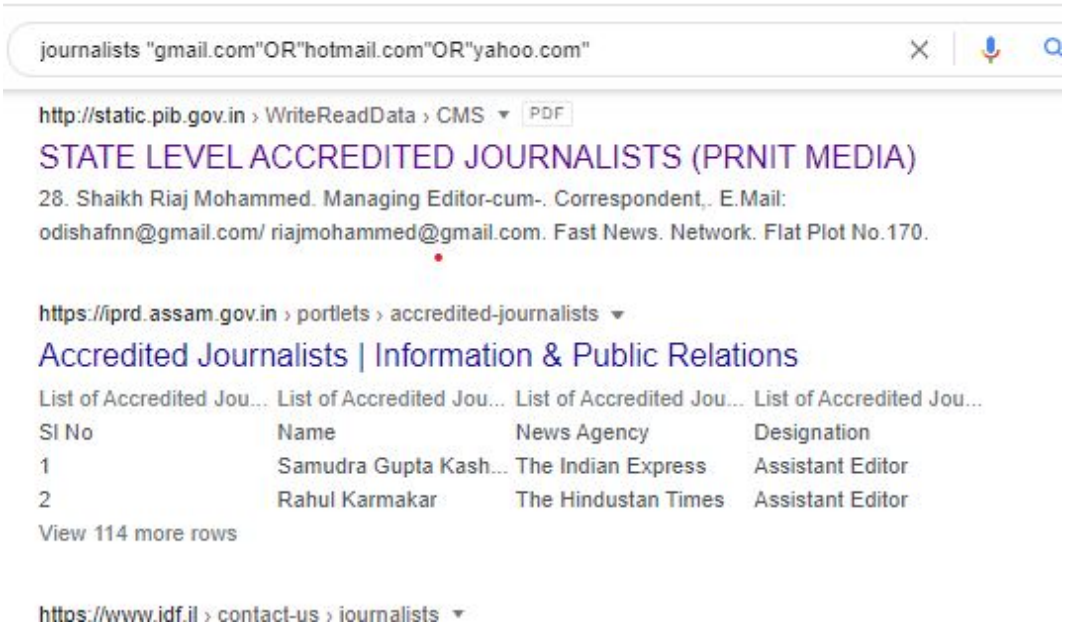
In the example above, I ask Annucapt to find me private investigators in New York via the Yelp directory. It gives me quite a few results but I don't have the email addresses. It doesn't matter because I get the addresses from their sites. When the search is over, I will copy and paste the url addresses and use them with Atomic email hunter which will find all the email addresses for me.

Annucapt is not alone in its market but as I have never used the others, I won't mention them.

The third one is a great little free tool that allows you to copy all the email addresses found on a page, regardless of the file format. You copy the page and paste into **Discoveryvip** .

To the right of the word 'separator', you click on 'new line' and then 'extract'.

Another great thing about the tool is that if I do a google search asking me to find addresses of journalists, I just copy the results from Google to the extractor.

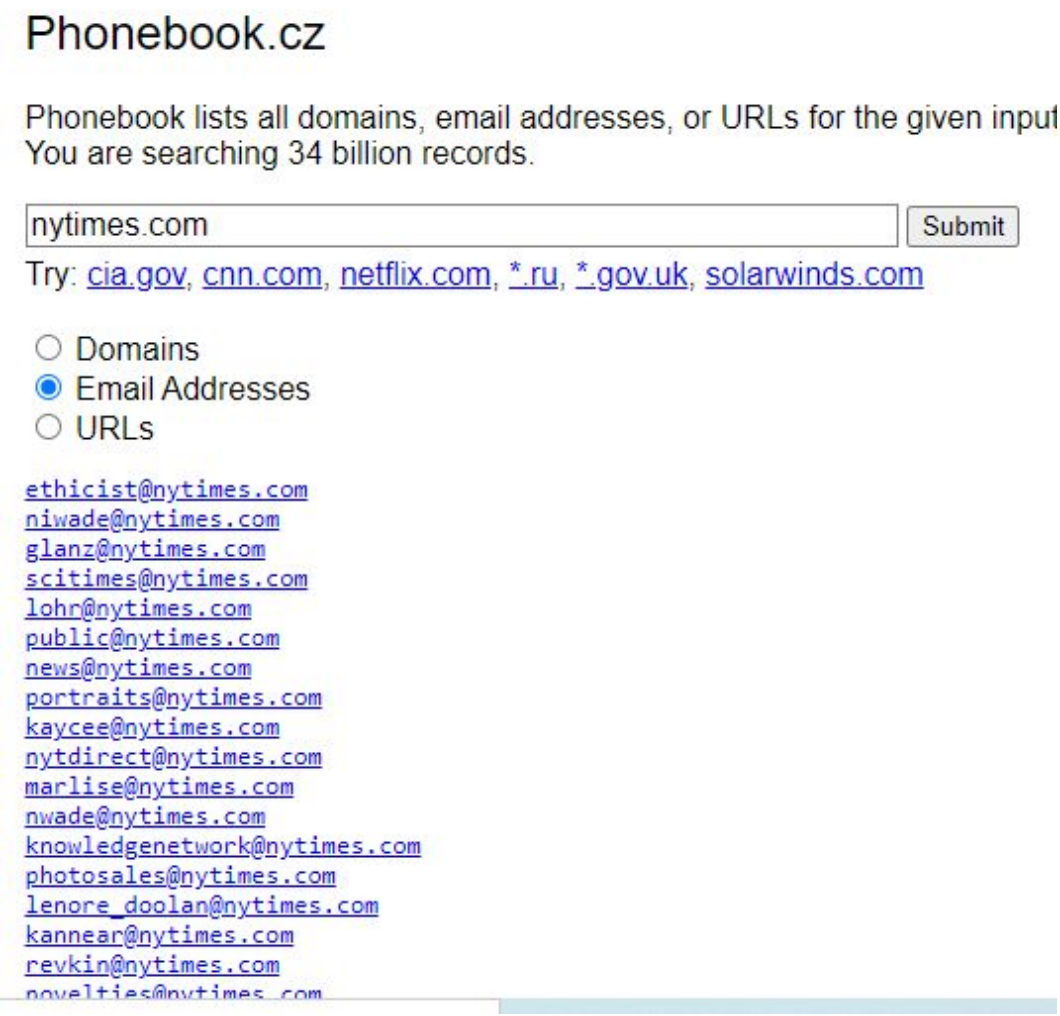


And voila, I've just created a database of 90 Indian journalists in a few seconds. Of course, this is just the beginning.

https://emailx.discoveryvip.com/

I have already mentioned https://hunter.io/ in the chapter on sourcing. As a reminder, with this tool, you can obtain many email addresses of people working in the same company.

The same goes for https://phonebook.cz/ which is free to a great extent and retrieves many emails from the URL of a site.



In this case I asked for the email addresses of the New York Times and I got 5,952 addresses which is a huge number. However, I have no information on the freshness of these addresses. Nor do I have any information on the functions performed by these people.

IX. Spying on social networks (socmint)

Social media intelligence (abbreviated to SMI or SOCMINT) refers to tools and solutions that allow companies to monitor different social media platforms and conversations, react to the different signals received on these social media, and synthesize these individual reactions to derive trends and analyzes based on user needs. You can of course do this to monitor your neighbor or your ex-husband.

Social media intelligence is about gathering information from these social media platforms, whether by intrusive means or not. This explains why the term 'intelligence' is used.

Social media sites offer many opportunities for online investigation, because of the amount of useful information in one place. For example, you can get a lot of personal information about any person in the world by simply looking at their Facebook page. This information often includes the person's Facebook connections, political views, religion, ethnicity, gender, age, his country of origin, personal pictures and videos, spouse's name (or marital status), home and work addresses, places frequently visited, social activities (e.g. sports, theatre and restaurants), employment history, education, dates of important events and social interactions. This information is obtained either directly or indirectly.

Social media intelligence is a sub-branch of Open Source Intelligence (OSINT). The data available on these sites can be either public or private. I am not going to get into the debate about whether these searches are legal or not. The debate is raging among researchers, mainly American but it can be said that if you wisely collect what is offered to you, it is legal. Of course, this chapter is not all wisdom.

The ease of access to information from social networks has its origins in various factors, mainly human.

- I have nothing to hide" is often heard. This is rather silly, because if you have nothing to hide, that's not why you want to show everything.
- Ego is a spy's friend. Many people, really a lot, find it very interesting to post pictures of holidays or meals - which are of no

interest to anyone - or to share articles from traditional or alternative media, giving the impression that they are defending a cause or being a journalist. All this for one more “like” As we saw in the chapter on human intelligence, ego is a sure ally of the intelligence officer. Don't misunderstand my slightly condescending words, the author of these lines is no different from any other human. We all have an ego, and it is a weakness that is easy to exploit.

- More and more often, profile owners seek to hide some of their information. We will see in this chapter that this is only an illusion of security.
- Finally, the technical aspect comes into play. There are many tools for collecting information on social networks. While it is not possible to hack sites like Facebook or LinkedIn, despite the promises of hundreds of online scammers, it is possible to circumvent certain security rules.

Types of social media content messages/updates online. For example, it is not possible to see other people's updates on Facebook if they restrict the visibility of a post to certain circles of friends or set it as "Just me".

Classifications of social media platforms

Many people use the terms social media and social networks interchangeably to refer to Facebook, Twitter, LinkedIn and related social platforms. This is not absolutely wrong, but it is not entirely accurate either, as their functionality and purposes are different.

Here are the main types of social media classified according to their function:

1. **Networking and talking to each other** : This allows people to connect with other people and businesses online to share information and ideas. Examples include Facebook and LinkedIn.

2. **Photo sharing:** These websites are dedicated to sharing photos between users online. Examples include Instagram and Flicker.

3. **Video sharing:** These websites are dedicated to sharing videos, including live video broadcasts.

The most popular is YouTube. Please note that Facebook and Twitter also offer a live video streaming service.

4. **Blogs:** This is a type of news website containing a collection of posts related to a theme or topic, organized in descending order by date of publication. The most popular blogging platforms are Word Press and Blogger, which is a Google spin-off.

5. **Microblog:** Allows users to publish a short paragraph of text (which can be associated with an image or video) or a link (URL) to share with others online. Twitter is the most popular example.

6. **Forums** : This is one of the oldest types of social media. Users exchange ideas and discussions in the form of posted messages and replies. Reddit is an example.

7. **Product/service reviews** : These websites allow their users to review any product or service they have used.

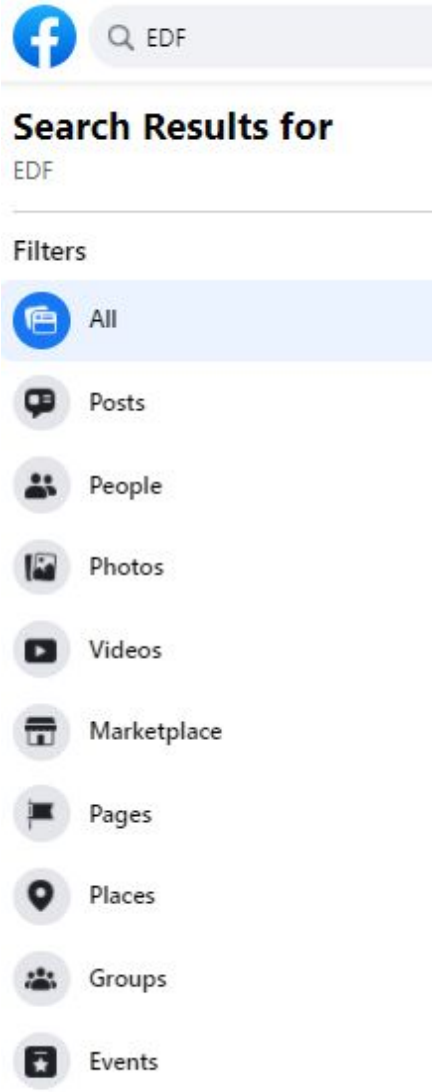
Now that we have a good understanding of the different types of social media, it is time to start talking about how to use the different tools and techniques to acquire information from these platforms.

1. Facebook

Facebook is the most popular social media platform with the largest number of users in the world. Facebook offered an advanced semantic search engine to search its database using natural English phrases and keywords. This semantic search engine called **Graph Search** was introduced in early 2013. In 2019, Facebook removed the search functionality via Graph Search. The power of Graph Search posed a real danger to the safety of some people but nature does not like a vacuum. This great tool allowed for queries such as: "single older woman from...to..., living in such and such a town". That's still a bit of fun, but "military man from the Paris area who worked in Afghanistan" is less fun. Once a technology has been created, it is very complicated to make it disappear. That's why tools to replace Graph Search have appeared. Not only that, but Facebook has also improved its search functions.

Let's say my search is on a fairly sensitive topic like nuclear power plants run by EDF.

People interact on social networks for different purposes. **SOCMINT** is interested in collecting all types of content, but the ability to do so depends on the level of privacy control set by each user when posting



I'm going to get a great harvest of information. Will I find the strategic nugget that will allow me to take over all the EDF power plants? Not at all as there is most likely no such a chance. If by chance a distracted or clumsy person were to publish confidential information (it happens, I saw a soldier announce an attack for the next day on his page) - the post would be deleted very quickly. It is by crossing information that your intelligence mission will lead to success.

In a very simple way, I will here access the posts published about the power plants, the people who work there, the photos and videos of the power plants, as well as the pages and groups dedicated to the nuclear industry and/or EDF, managed or not by EDF. Whether it is for groups, people, pages or photos, I still have the possibility each time to refine the search according to different criteria.

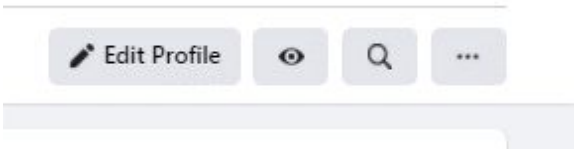
On the left side of the screen are the filters. You can use them to narrow down your list of results and make it more manageable. Following Facebook's radical redesign in 2020, the old default filters are no longer available. They have been replaced by a new list of 9 filters. The new filters each have a specific purpose and have dedicated sub-filters that allow you to refine your results. Facebook has become a search engine in its own right.

The new filters are: posts, people, photos, videos, markets, pages, places, groups and events.

If you search for a person, it works even if you are not friends with them.

In all, you will be able to see photos taken by the person themselves or others, but you will not be able to see what events the person is attending, whether they are a member of certain groups, or the important thing, read their posts. Often you will not be able to see their friends list, which is very important in an intelligence mission. We will see later that it is still possible to access all this so-called confidential information.

To read a person's posts, the ones they have published on their page or on someone else's page, there is a trick. This trick works partially, even if you are not friends with the person. When you go to the target's page, at the top right of the page, under the profile picture, you find this:



You click on the magnifying glass. If the magnifying glass is not visible, you click on "..." and you will see the magnifying glass. Type in the name, surname, a combination of both or a nickname of the target.

You will get different results. Previously invisible posts are now accessible. You can sort them by years or by recency. There are many online services that simplify the process of acquiring/analyzing Facebook account information. Often you will need to know the Facebook ID of your target.

https://lookup-id.com/ will do this very quickly. Beware that the result appears at the very bottom of the page, you might think that the engine is not working.

For example, if you need to know if a person is a member or administrator of a group, there is an extension for Chrome to get the information. If you use the Google Chrome browser, you can use the "Multiple Tools for Facebook" extension. This extension focuses mainly on your own profile, but it has a really interesting feature. Make sure you have obtained your target's profile ID before following these steps. Once the extension is installed, go to the menu and choose "tools" from the left-hand menu. You will then see a search bar in which you will find the profile ID number you are connected with. Delete this number and replace it with the ID number of your target. Click on "Search" to see the groups of which your target is a member or administrator.

The downside of using this Chrome extension is that it is possible that your profile will be temporarily banned because Facebook detects it. This has happened to me several times after intensive use. It seems that in case of industrial use, your profile can be permanently banned. Either you use this extension carefully or you have a fake profile that you can do without.

Although it sounds a bit folksy, Facebook is the most widely used intelligence tool. Here are some of its uses.

- **Resume check** . During a CV check, the entire Facebook profile is scrutinized. No need to be too paranoid either. If you are seen in a swimming costume on the beach or a bit drunk during a party with friends, this is not what will make you miss out on the job of a lifetime. On the other hand, and notice how frequent this is in your circle, conspiracy or xenophobic comments will not pass. Of course, it all depends on how virulent your writings are. A close friend, working for the city, received a rather acerbic letter following one of these posts because it "damaged the image of ... » There were no

serious consequences for him or his career, except for certain resentment towards his employers.

- **Espionage between partners** . This is extremely common. One partner wants to know the intentions of the other. How beautiful is the new house you bought in southern Spain! Your holiday in the Maldives. Your beautiful Porsche. If you're planning to change your life, it's likely to show on Facebook. Not only because of your clumsiness, but also because of your friends' comments
- **Partner validation or pre-merger/acquisition investigation** . The page of the potential partner is thoroughly investigated, as are those of the director and senior managers. So are their Relationship.
- **Competitive analysis** . This is the same as the previous point. With the added bonus of intensive use of digital marketing tools. These tools are not about the people but only about the target company and its sales and marketing policy.
- **In the search for people,** it is the number one tool. I'm not talking about searching for criminals, I don't know anything about that but ordinary people, who are wanted by a family, or a solicitor, and who are not in hiding or those who have unpaid debts, who have moved to another country and think they are out of reach. A simple photo will identify you through a number plate, the presence of a public building or a simple shop sign. Your friends will unwittingly and unknowingly refer you to an experienced investigator.
- **Credit investigation** . When it comes to a business, it is relatively easy to find out whether it has the means to repay its debts. In the case of an individual, there is little public information. Before taking legal action, a creditor will want to know whether the debtor is solvent. The number one key (and I stress, when it comes to an individual) is to kn ow whether the debtor has a job, real estate a personal car etc. Facebook often helps answer these questions (or gives you leads to investigate further), whether through the Facebook profile, photos, or comments from friends ("congrats, congrats, on your new promotion!"). Most people who owe you money have a Facebook profile.
- **Military intelligence** . It seems absurd to think that Facebook could be a military intelligence tool. For a skilled and experienced analyst, Facebook is an incredible source of information about an ongoing

operation. If I want to get information about the French military deployed in Mali, it is unfortunately very simple. I'm not just going to use Facebook, but on this site I will benefit from photos and videos taken by the army itself, by journalists and soldiers.

Using keywords like "Mali legion", "operation Barkhane", "French military Mali", "legionnaire Mali", the names of different units that are on the ground and whose names are mentioned everywhere. I will find thousands of documents. Each document will be quite innocent on its own. It is the impressive collection of resources that will allow me to identify: the units on the ground, the armament, the defense systems, and the men involved, with the possibility of finding their private address. The photos and videos are commented on. Most of them are commented on by people who congratulate or insult the military but have no connection with the field. So it's all meaningless information but very often comments come from the soldiers themselves. They give information that may not seem very sensitive, but they allow the identification of the units involved and, above all, they give their names.

Tools and tips

a)Create a fake Facebook profile

This gives you the opportunity to search Facebook at lower risk and also to create a legend if you want to become friends with a target. To do this, it is best to be untraceable and this is quite possible.

When you sign up, Facebook will ask you for an email address. It's easy to create one, but the best thing is to have a disposable address that self-destructs after a few minutes. When you go to https://10minutemail.com/ , you get an address for 10 minutes and an inbox. You register on Facebook, give your disposable address, then go to your temporary inbox to reply to the confirmation email from Facebook, and that's it. 0 traces.

If Facebook rejects your temporary address, don't panic. This is private intelligence. You never need the same level of privacy as a government official. You cannot use your personal email address to create a fake account, you must create a new one that you will only use for the fake account.

Avoid using this email address on services that could be traced back to you (e.g. in your bank account login details or a contract for an online service).

Use a different email provider than the one you currently use for your Facebook account. For example, if your account is linked to a Gmail address, try creating a Yahoo or Outlook account for your fake account. Or better yet, a Yandex.ru account.

Create a credible email address and use the same name you will use for your Facebook account. If Facebook thinks the account is fake, you may be asked to provide a photo ID with a picture of yourself to identify yourself.

Then you go to https://thispersondoesnotexist.com/ which is a site that generates photos of people that don't exist. You restart the site until it offers you a photo that you like. What is the point? The same as in the previous point. You can't trace the photo with a reverse photo search program, since the person doesn't exist.

This is a photo of a person who does not exist. Isn’t it pretty convincing? Don't use photos found on Google because if a user notices, your account could be closed.

At this point, you have created a fake untraceable profile. Actually it is not untraceable but it will be difficult to trace. Next, you will need to create an identity. This depends on what you want to achieve with your fake profile. Choose your name carefully.

Be aware that almost everyone who creates a fake name keeps the same initials. Add your age, interests, date of birth, job, schools, depending on

your purpose and avoid being projective, i.e. creating a fake identity from the real one.

If your new profile is created based on a particular person you want to be friends with on Facebook, consider creating a profile that has something in common with that person's world. We like people who are similar to us. For example, you have a 40% greater chance of being accepted by a person if you have the same name, or the same town, or the same school, the same job etc .Don't overdo it though.

Start inviting friends. Even in this day and era, many people accept people they don't know as Facebook friends. At the same time, start posting because a profile with no posts, no friends and that was created yesterday, is not exactly sexy. It is possible to use real, inactive profiles, but this is even more suspicious because the only advantage here is that the profile has a past. The disadvantage is that the content will probably not look like the person you are supposed to be with your fake profile.

Many people have a fake profile not for the purpose of harm or spying but simply to ensure their safety. It's not illegal at all as long as you don't impersonate anyone.

b)Identify your target's Facebook friends

If you are conducting a background check on a future business partner, you may want to know their connections? Today, many people hide their friends list, eventually leaving it visible to their relatives. This is totally unnecessary. You can't hide your Facebook friends unless you never post anything.

To identify a target's Facebook friends, you go to each of your target's publications and click on the "like". By going to the different publications of the target, you should be able to get a nice list of friends, probably not the whole list, but certainly those in the close environment.

c)Using external tools for Facebook search

Sowdust is a tool in constant development. It allows Facebook searches to be conducted by combining different criteria. It allows you to conduct chronological searches, find photos or messages published or tagged by a person, and in some cases, locate an image.

https://sowdust.github.io/fb-search/

Whoposted allows you to search for information on specific dates.
https://whopostedwhat.com/

FBsearch is another tool for searching on Facebook. Very simple, but basically does nothing more than what you can already do via the Facebook search bar, which has been considerably enhanced.
https://fb-search.com/search

d)Using Facebook character recognition

In concrete terms, if something is written on a photo, a name, a license plate, Facebook will find it. For example, if I search for a vehicle with the registration number "KLT666", here is the result:

Warning, before you think you'll find the driver who smashed your car, this only works if the photo of the plate exists on Facebook. The probability is low, although it's always worth a try. In the Facebook search engine, you type in the license plate number, and then click on "photos".

e)Find someone on Facebook by email or phone number

Facebook is a great tool for finding information about people. With over 2 billion monthly users, the chances of finding someone's profile by their last name alone are slim - especially as they may not even use their real or full name! Fortunately, there is another option: you can search for a person's profile by typing in their email address or phone number. To do this, simply log into your Facebook profile and enter the email address or phone number of the person you are looking for in the search bar. Then click on the "People" tab at the top of the page.

This search only works if the user's email address, or phone number, is set to be publicly visible in their "About" section. If it is not, it will not appear in the search results but it's worth testing. Also, as far as the phone is

concerned, you will very often be able to locate it if the person has, for example, a contact profession, or a business.

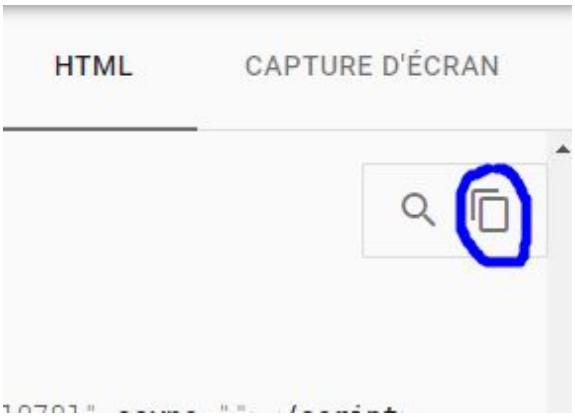
2. LinkedIn

Is your competitor active on LinkedIn? Probably, but apart from its great sourcing functions, LinkedIn is less interesting for competitive analysis than other sites. Simply because your competitor does not sell his products here. Apart from competitive analysis, LinkedIn is of course a source of information about people. You will get data, unverified, about the person's education and different jobs. Often in our jobs, we don't want to be identified. However, on LinkedIn, when you visit a profile, the target will be notified that you are there. This is a default setting. It is possible to change your settings so that you are not identifiable.

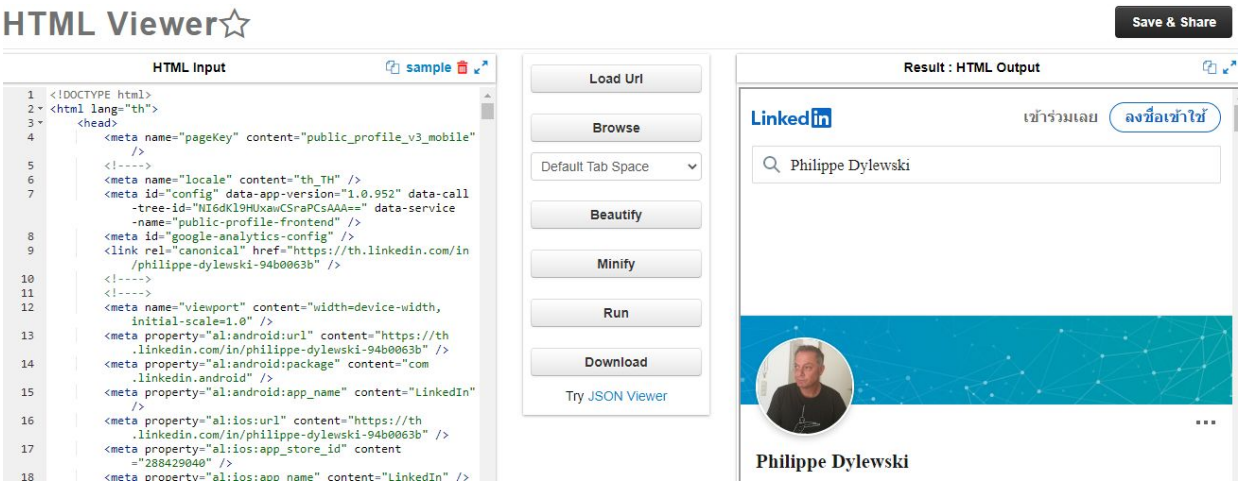
Click on the "You" icon at the top of your account home page and then click on "View Profile", click on "Preferences and Privacy". You go to 'privacy', in the section 'how others see your activity on LinkedIn', click on 'profile view options'. A drop-down list will open, this is the "Select what others see when you view their profile" module that will appear. You click on "Anonymous LinkedIn User". The person will know that their profile has been visited, but will not be able to identify you. If you are highly paranoid, or for some reason you need to visit a profile regularly and don't want to arouse your target's suspicion, it is quite possible to view a profile without the person knowing that their profile has been visited. It just takes a few minutes.

To begin, you type your target's name into your usual search engine, along with the word "LinkedIn". You see your target's profile at the top of the page. Go to the title of the link and use the right click of your mouse. Click on "copy link".

Then go to https://search.google.com/test/mobile-friendly , which is basically a way of finding out whether a web page is compatible with your phone. You copy the link into the search bar and you will see the LinkedIn profile of your target. But as the profile will be incomplete, you click on "html" at the top right of the page. The sequence of codes that appears is not very soluble in my mind. It is difficult to use. So I click on the 'copy' button.



Then you open the page https://codebeautify.org/htmlviewer and paste the information into the clipboard. Finally, you click on the "run" button and you get the target profile.



Getting back to your competitor, start by searching to see if they have a LinkedIn account. If you can't find it, you've either searched incorrectly (try again!) or your competitor isn't very dangerous.

Do they run ads on LinkedIn?

To access ads on a LinkedIn business page, go to the page and look for the "Ads" tab on the left. Click on this tab and you will see a list of ads associated with the page. Take note of the ads it runs and see what you can learn. Review the creative and copy you see for ideas you can incorporate into your ads.

Which ads get the most interest?

You can't view comments or interactions on LinkedIn ads directly from the ads section, but you can view this information in a roundabout way.

Click on the three dots at the top right of a message and select "Copy link to message". Then paste this link into your browser to view the message in question, along with any comments.

3. Twitter

Regardless of your industry, you probably have a competitor on Twitter. By following their strategy on the platform, you can glean valuable information for your social media marketing strategy just by looking closely at their followers.

One of the best ways to find out what works for a competitor on Twitter is to watch what they do. You don't even need to follow them directly. Just create a private Twitter list (visible only to you) and add your competitor to it. If the competitor has more than one main Twitter account, or if all their employees are on Twitter, include them too. This way you'll have a stream of incoming information telling you exactly how they're managing their Twitter strategy. You can create a private Twitter list on Twitter by selecting "New List" in the sidebar of your homepage. In just a few minutes, you'll start to see the type of content your list is sharing.

By searching on your competitor's username, you will be able to see the conversations they are having with their clientele. This way you can see what their clientele (or detractors) like or dislike about them. You can create a search in Twitter by simply searching for your competitor's username and using the "Save this search" option.

Are you interested in getting an overview of your competitor's customer list? Of course you do, otherwise you wouldn't be here. Services like **Tweepi** allow you to view their list of followers and sort it by number of updates, number of followers and other parameters. You can essentially find out who some of their most active and influential customers are. https://tweepi.com/

Since you and your competitors are going after the same audience, tracking their movements can be very useful in developing your own strategy.

You can get solid information by checking who your competitor is talking to on Twitter and how active they are on the channel. By default, Twitter only

shows you someone's outgoing tweets, not their replies. To see the replies, go to their Twitter account and click on the "Tweets & Replies" option. You can then see all the conversations they are having and with whom. Follow the people they talk to.

If you identify some key partners that they regularly engage with, research both your competitor and these people to find historical data on their conversations. An excellent tactic is to create Twitter lists.

Lists can be public or private, but for monitoring the privacy of competitors, this is the best solution.

To create a list via the web:

Click on your profile icon to display the drop-down menu.

Click on "Lists".

Click on "Create a new list".

Select a name for your list, and a short description of the list. Then choose whether you want the list to be private (accessible only to you) or public (anyone can join).

Click on "Save list".

Following some relevant industry hashtags can help you learn about new players in the market that might be worth exploring. Twitter has a built-in search function in the top right corner of the screen. You can add advanced search operators - similar to Google's - to your query, dive deep and return specific results. To begin your search of the Twitter database, it's a good idea to go to the Twitter Advanced Search page at https://twitter.com/search-advanced. From this page, you can customize search filters based on specific date ranges, people and other items.

1. (-) is used to exclude specific keywords or phrases from the search results.

2. To search for hashtags, use the (#) operator followed by the search keyword. For example: #Dior

3. To find tweets posted in a particular language, use the "lang" operator. Dior lang:fr

4. Use the keyword (images) to return tweets that contain an image. Here is an example: OSINT: images filter (this will return all tweets containing the keyword OSINT and containing an image).

5. To return tweets containing a video, use the keyword (videos). Here is an example: OSINT: videos filter

6. To search for tweets with negative reactions, use the following symbol :(For example: Dior :(will return all tweets containing the keyword Dior with negative attitudes.

7. Limit your searches by specific dates with the operators using since: and until:

Example: "Dior since: 2020-03-01 until:2020-12-31

8. To search for tweets associating two words, you use the AND operator:

Dior AND: Boston

9. One or the other. You use the OR operator:

Dior OR: Gucci

10. Filter or exclude. With the filter: operator, you can filter the tweets according to several criteria:

Verified: show tweets from verified accounts

Follows: show tweets from people you follow

Replies: only reply tweets

Retweets: only retweets

Links: only tweets with a link

Images: only tweets with an image

native_video: only tweets with a video

For example, to search for links about Dior, use this query: "Dior filter:links".

By using exclude: instead of filter:, you exclude the above criteria.

4. Amazon

Are you losing sales to your competitors on Amazon and having trouble understanding the reasons? What if you could spy on your competitors on Amazon and see what pricing strategies they are implementing to ensure their success? Using the Amazon product research tools available on the market, you can easily perform a detailed comparative analysis between you and your competitors.

To stay ahead of your competitors, the first step is to identify who they are. The next step is to find out what your competitors are doing, which is often a bit more difficult than just doing a Google search.

Here are some factors to consider:

- How are they better or worse than you?
- Do they have a wider range of products?
- What is their average selling price?
- What about their reviews, sales and rankings?

With an Amazon search tool like **BigCentral** , you can easily examine your competitor's performance at a glance. BigCentral's Best Sellers Analytics table gives you access to the competitor's overall performance with up to 120 days of historical data, as well as their daily sales volume and revenue.

Another way to effectively spy on Amazon's competitors is to set up an alarm. BigCentral's alert system will automatically notify you of any changes in your competitor's inventory, pricing, reviews, ratings, revenue and more.

BigCentral is good. You can try it for a fortnight but at $50 for a basic subscription, your presence on Amazon has to be more than just selling three used books a month. https://www.bqool.com/

Another important reason to actively monitor Amazon's competitors is to find out which of your competitor's products are eating into your revenue. Your competitors are not only those who sell the same products as you, but also other sellers who sell products that can be purchased in addition to what

you sell. It is therefore essential that you track the performance of your competitor's products.

With product tracking, you can easily identify your competitor's best-selling products and monitor product price, reviews, sales, profit margin and inventory levels. With this in-depth analysis, you can implement action plans to stay ahead of your competitors.

The reverse ASIN function shows you which keywords your competitors are already successfully using, search volume, average sales, click-through rate and performance metrics. The Amazon Standard Identification Number (ASIN) is a product identification code used by Amazon.com. Every product sold by Amazon and its affiliates has a unique ASIN number (definition, Wikipedia).

Trendle helps you with this task with a reasonable budget, ranging from free for a fortnight to a subscription that starts at $10 per month. https://trendle.io/

How can you find out when your competitors are running promotions? Here are some ways:

Check out the "Today's Deals" section on Amazon.

Visit your competitor's website to see if they are offering discounts or deals.

Check social media, blogs, newsletters, affiliates, etc. Many sellers also post their special offers on customers pages.

Amazon is a very competitive and ruthless place. You lose an edge in a very short time. Your competitors outrank you within hours. Your customers celebrate your glory or your downfall in two clicks. If there is one place where information is a matter of survival, it is on Amazon.

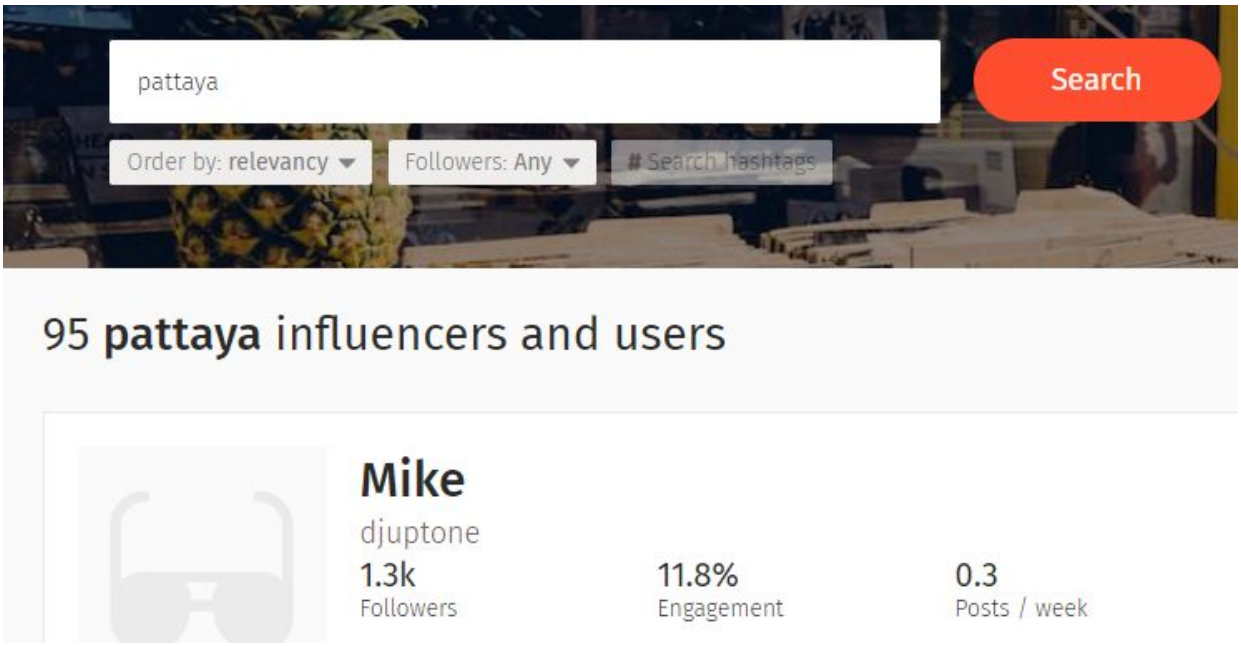
5. Instagram

Instagram is the social network for images, whether they be photos or short videos. At first sight, it has no interest in intelligence. Spying on teenagers pretending to have fun by the pool won't add much to your competitive analysis. Today, Instagram has become a must for brands and businesses. It's the place to get known and recognized. We have already seen how to track

ads on Instagram. There are still two other important categories: followers and influencers. Followers are those who have decided to follow a user. We are interested in them because they are the real pulse of a brand or company. We are interested in what they like, what they don't like, what they say about it and who they are.

An influencer is a kind of star intermediary between a brand and its audience. Because of their fame, influencers have the power to "guide" consumers in the right direction. They have much more credibility than an advertising campaign because the trust factor works in their favor.

For example, if my client is a tour operator that organizes trips to the glittering city of Pattaya, Thailand, I would want to know the top influencers related to this topic. This is what **Searchmybio** does for free.



For each thematic search, I get a list of the main influencers. With their number of followers, the engagement rate (percentage of followers who interact with a publication) and the number of posts per week.

https://www.searchmy.bio

With **Social Blade** , I can follow my competitors on Instagram and know everything about their evolution almost in real time: number of followers, engagement rate, pages followed by the brand, average number of likes and posts, all accompanied by very clear graphs. What is very interesting about

Social Blade is that the site does the same job for other social networks such as Facebook, YouTube, Twitter or Tiktok.

FACEBOOK STATS SUMMARY / USER STATISTICS FOR DIOR (2020-12-14 - 2020-12-27)

DATE		LIKES		TALKING ABOUT	
2020-12-14	Mon	–	17,390,212	–	279,074
2020-12-15	Tue	+4,253	17,394,465	+18,959	298,033
2020-12-16	Wed	+3,510	17,397,975	-12,699	285,334
2020-12-17	Thu	+3,503	17,401,478	+17,887	303,221
2020-12-18	Fri	+3,692	17,405,170	-15,929	287,292
2020-12-19	Sat	+3,817	17,408,987	+8,717	296,009
2020-12-20	Sun	+3,737	17,412,724	+16,236	312,245

https://socialblade.com/instagram

X. All about your business partners

These are your customers, your agents, your distributors, a merger or acquisition project. For the most part, the methods are the same as in the chapter on information about your competitors. I recommend that you read this chapter, as it contains a series of tools that will be useful for your project. However, there are some differences. If your competitor is in financial difficulty or has a reputation for being a rogue, there is no problem. In the case of an alliance, this is a major problem.

Thanks to the databases, you obtain all the information on the company's finances, its credits, its payment deadlines, etc. Of course, financial analysis is essential. You have studied its marketing strategy and that's fine.

All this information has one negative point in common: it gives you information about the company's past. When you read a balance sheet, it is a balance sheet from the past. It does not tell you what is happening today. Of course, in the case of a takeover, you are free to ask for the interim results of the current year but you yourself could have ever already arranged your results in the past to make them look as good as possible. We're not talking about fraud, no, not at all! We are talking about embellishment. You have come here to visit the company and see how dynamic it is.

But your future partner had been informed of your visit. When you receive important people, you go to great lengths, right? So do they. Temporary workers were hired for the day. Family and friends jostled each other all day to give the impression that the guests were spending in droves. The phone keeps ringing. Trucks roar . The machines turn red. Social networks proclaim what a gem your future partner is.

This type of scam was one of the most popular in Thailand until early 2020. Thousands of French speakers arrived each year in the Land of Smiles with the dream of building a new life in the sun. Take over a small business, a hotel, a bar or a restaurant. The pigeon is looking to make contact with French speakers who have been in the country for a long time. It's warm, the atmosphere is so nice. Very soon, he is informed that a great bar is up for sale because the owner wants to return to France for family or health reasons. The appointment is made in the bar in question and it's crazy. You

practically have to push the banknotes into the till with your foot. It's a party, everyone's having fun, people are eating and drinking. The pigeon is baited, he has found the deal of the century, he is treated like a king, presented to the customers as the future owner. He has never seen anything like it. There is a substantial takeover price and a lease to take over, but it's still acceptable. After two or three drinking sessions where the pigeon already sees himself as a prince of the night, the business is done. Everything goes wonderfully well until the day of the opening when there are just three lost customers. At about 11 p.m. a police patrol arrives and tells the pigeon that he is not in order of this and that. He quickly understands that he has to pay. Not much, because here we don't kill the pigeon, we cook it on a low flame. The real problem is not corruption, because in the end it is only a small contribution to the work of the police and your safety is guaranteed. The real problem is that all these party people are not there and for good reason, as they are now boozing in the new establishment opened by the former owner. The former owner is happy to do the pigeon a favor by taking over his brand new establishment for a very modest sum.

You think you can't be fooled by the poppycock of adventure-seeking retards? Then you'll be fooled. I can already hear the cooing. Heavens, is that a pigeon? The only way to avoid being fooled is to have the humility to recognize that it is possible.

This scam is not so easy to detect. Indeed, the business exists. It works really well and has all the necessary authorisations. The success is unquestionable, as the pigeon has seen for himself during some crazy nights. This is where human intelligence comes into its own because the pigeon did not ask about the reputation of the seller. Yet, in the context of this case, this was very easy to do because the pigeon would have inevitably fond a compatriot to tell him to beware, that the seller is known to swindle his compatriots. He did not wander around the neighbourhood to see if a new bar was about to open.

What you can hardly know is whether anything significant has happened to your potential partner in the last few months but it is possible.

Whether your future partner is in your country or abroad does not make much difference. The only difference is who will do the intelligence work.

a) **For a publicly accessible business**

Send a few people to pretend to be customers during the week and at weekends. Check that the key people are still in place. For example, that the restaurant you are considering taking over has not seen its chef resign to open his own establishment nearby. Or that the owner is going to open something new in the neighborhood.

Someone will be on the lookout to see how many people enter the restaurant on one day. A weekday and a weekend day. This person will count the number of bags and calculate the supposed turnover with this information. By the way, I would point out that this is exactly what some finance officials do.

The surveyor will walk around the immediate vicinity of the shop and seek to engage in conversation with local residents. A key person will be the postman because he knows everything. Until a few years ago, many estate agents paid postmen to be aware of potential deals. Well, maybe they still do.

You investigate the owner thoroughly via social networks, the press and the media in general. If possible, you contact the suppliers of the business under some pretext, to get information about the payment habits of the target.

Finally, via a private investigator, you invest a small amount of money to find out everything about the owner's assets and creditworthiness in real time.

Normally you don't have access to the criminal record, except in the US, but knowing that he was convicted 25 years ago for selling pot or stealing a car is not of great interest. If he has committed a serious offence in recent years, you should have a record of it in the media.

b) **Fora larger company or a company not open to the public**

Some of the previous points are relevant: personal credit check of the manager(s), contact suppliers, test the product/service, the quality of the reception, check that the main managers do not have projects incompatible with yours. If there is production, count on one or two days for what comes out of the company. Take advantage of this to pay attention to the condition of the trucks.

If it is service provision, contact clients to find out if there have been any recent changes in service provision.

When checking the company's reputation on social networks, pay particular attention to the date of publication because if the owner seeks to

misrepresent itself, many of the abnormally positive posts will be very recent.
During lunchtime, send someone to places where staffs are having lunch and either just listen in on the conversations, or if the interviewer is clever, get involved.
Check on LinkedIn to see if any key managers have been away from home lately. This is done by searching for people who are currently working in the company or who have worked there. If you see that people who have worked for the company have changed jobs en masse in the last three months, raise a red flag in your mind.
If you are planning a partnership with a company that has branches and shops, consider arranging visits and look around to see if any new competing companies have recently set up in the area.
You certainly don't want to work with a company or people suspected of financing terrorism, banned from banking, on international money laundering lists, wanted fugitives by Interpol, with assets frozen in various countries, or on the FBI's wanted list. This would be bad for your business. Financial institutions are obliged to check that their clients are good clients.

There are hundreds of lists around the world with the names of very unsavory people. You can't go through all of them, because you'd be stuck for weeks. Fortunately, there are many companies that centralize the information for you. Often at gangster rates. **KYC2020** is the best in the class. Not only can you test their services for free, but after the test their prices are very competitive. The PDF report you receive gives you a simple yes or no answer. Then the document explains why it is not a good idea to work with this nice businessman with whom you were planning a solid cooperation.

Record #: 3	
List Hit: interpol	
Match Attribute: First Middle Last Name (Match Confidence# EXACT),	
Match Confidence: EXACT	
Source Document	
dob	10-24-1952
nationality	MX
name	RAFAEL CARO-QUINTERO
gender	M
url	https://ws-public.interpol.int/notices/v1/red/2013-43755
crimetype	1) Commission of violent crimes in aid of racketeering (4 counts) 2) Conspiracy to commit violent crimes in aid of racketeering 3) Conspiracy to kidnap a federal agent4) Kidnapping of a federal agent5) Felony murder of a federal agent

I am shocked to learn that Rafael is wanted by most of the world's police forces for racketeering, murder, conspiracy and kidnapping. Now you can't say you didn't know. https://www20.kyc2020.com/

While you're at it, also check the list of Europe's most wanted criminals on the Europol website. https://eumostwanted.eu/fr

The **GTD (Global Terrorism Database)** is the world's largest directory of terrorist events, listing almost 200,000 attacks since 1970. You will find the name of every person involved and identified. https://www.start.umd.edu/gtd/

The UNITED NATIONS SECURITY COUNCIL offers a search engine for people or organizations affiliated with international terrorism.
https://scsanctions.un.org/search/

To conclude this chapter, I present a classic case. It was a very simple job in the summer of 2021, a wood importer contacted me. He had received offers from 8 Ukrainian suppliers and as the prices were very low, he had some doubts. He didn't want me to investigate each company in detail, but to have a look around in case I found something odd. This was important because in order to place an order, he had to pay for the delivery before it could be sent.

For each entity, I checked:

- The date of registration of the website.
- The registration of the company in the Ukrainian Trade Register.
- That the main phone number on the website is not found on dozens of other websites.
- The email address provided by the site to see if it is found on scam sites.
- For each domain name, I looked to see if there were online reviews and a presence on social networks.
- Location on Google map the official address provided on the website.Finally, I looked to see if the company's representative had an existence on social networks. For this, I used the website deepl.com which offers almost perfect translations.

After my fifth report, the client told me that there was no need to continue and that I could send my invoice. All the sites were bogus, without exception

and unheard of. Almost all the sites had just gone online. Most of the companies did not exist. The addresses ended up in empty lots...

The above procedure does not require you to be a graduate of the FBI Academy. It takes 30 minutes to an hour of work and will save some of you a lot of money. Of course, in some cases, further investigation may be useful. The purpose of this chapter is to show you that it is very easy to avoid most scams. Not all of them, of course, but most of them.

XI. The Dark Web

The dark web refers to encrypted online content that is not indexed by traditional search engines. The dark web is part of the deep web, which simply refers to websites that do not appear on search engines.

Specific browsers, such as **Tor** , are needed to access the deep web. Many dark web sites simply provide standard services with increased anonymity, which benefits political dissidents or people in general who are trying to maintain their privacy. Obviously, illegal drug sales, porn for all tastes, stolen data sold at auction and weapons attract the most attention from the general public. The dark web is as much a dream as a thrill.

https://www.torproject.org

The Tor Project is a non-profit organization that conducts research and development on online privacy and anonymity. It is designed to prevent people including government agencies and corporations from knowing your location or tracking your browsing habits.

Based on this research, Tor offers technology that bounces traffic from users and websites through "relays" run by thousands of volunteers around the world, making it extremely difficult for anyone to identify the source of the information or the location of the user.

Its software can be downloaded and used to leverage this technology, with a separate version available for Android smartphones. As in the early days of the internet, the dark web has also gained a reputation as a haven for illegal activity. This reputation is well founded, but only in part because the dark web is also a place of privacy preservation and this book shows you how fragile it is.

Download Tor from the above link, once download is complete click on the setup. Tor browser will then ask you to choose a language for the browser, make your choice. Specify the installation folder for Tor on the next screen. Tor will then be installed in a couple of seconds in your system. When you run Tor, it will ask you to either “Connect” or “Configure“. Clicking on Connect is the fastest and simplest way to land on the Deep/Dark web.

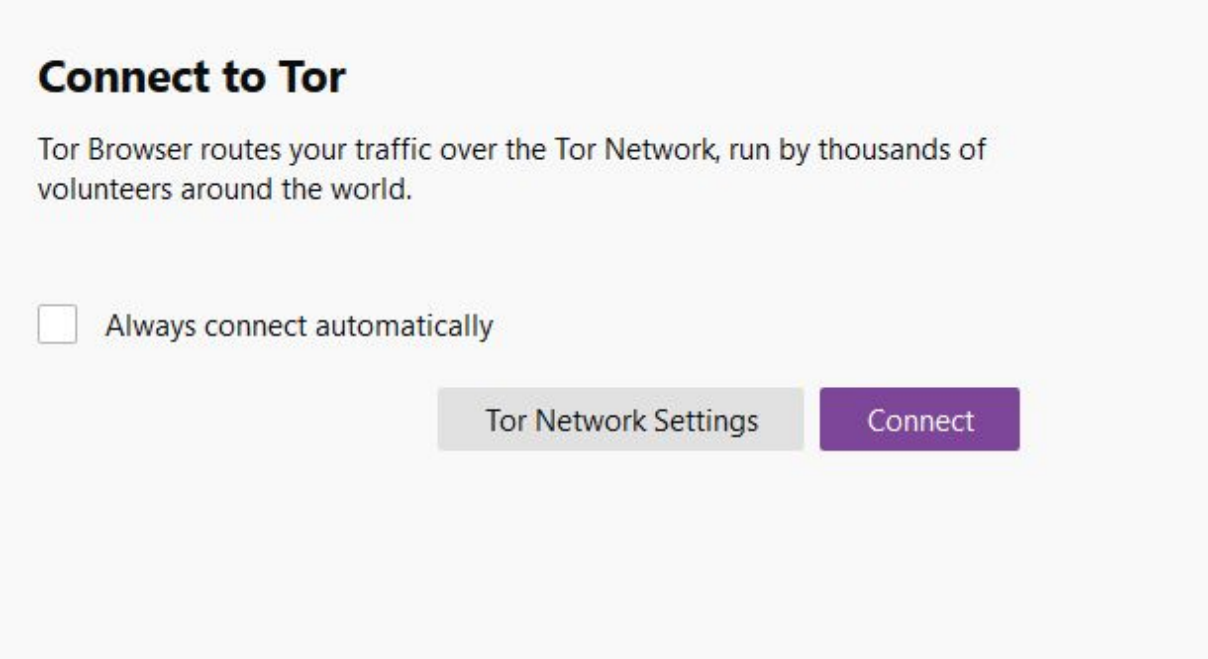
Once you've installed Tor, you need to amp up its security before accessing the deep web, and here's how to do it. On the extreme right of the Tor browser, you will notice a "Shield" icon. Click on it and finally, just choose "Safest" from the list of options available.

This will slow down your browsing. If there are times when you are unable to watch videos, you can change the security level of your browser if you are sure which "onion" site you are on. You should always be connected to a VPN before you go on Tor. I insist on always but if you think the worst is yet to come, then go to the Darkweb without a VPN. Wandering the Darkweb without VPN protection is like swimming in a pond full of crocodiles and thinking they've probably already had lunch.

If you have the idea to register on a site found on the Darkweb, use a fake identity created for the occasion.

You also need a secure email address. **Protonmail** is an E-mail provider, a platform which lets you create, send and receive E-mails and files in total security and discretion. It is Swiss quality. Unlike Gmail, Yahoo or any of those other mainstream E-mail providers, Protonmail is anonymous, secure and is off the govt.'s reach. It's an E-mail provider which protects your privacy and security and that's what makes it special. https://protonmail.com/

Unplug all your external devices like portable camera, printer, smartphone and cover your laptop camera. Close all running applications at the time of deep web access.



When you click on the Tor icon on your desktop, you still have to go through the connection process. Click the "connect" button and voila, now you're ready for the journey.

Much of the content on the dark web is very amateurish. Maybe that's what makes it fascinating, a bit like adolescence. The dark web is still evolving, and its costs and benefits are not yet fully known.

The dark web, like the internet before it, is often accused of horrific crimes, such as child abuse and murder for hire. However, these crimes existed long before the internet or the dark web. The difference, and it is a big one, is that with the dark web, it is easier to avoid being caught. It is essential to avoid confusing the dark web with the cryptocurrencies often used to make purchases there. The dark web facilitates the creation of and access to websites that offer a high degree of anonymity for all concerned. Many of these sites contain only information, with no possibility of buying or selling anything. It is true that cryptocurrencies, such as Bitcoin, are often used for transactions on the dark web. However, it is not necessary to use the dark web to use cryptocurrencies.

The dark web and the deep web are also often used interchangeably and incorrectly. The deep web includes all the pages that do not appear when you search the web. The dark web is only one part of the deep web, which also contains everything that requires a connection, such as online banking,

payment sites and file hosting services. The dark web is a subset of the deep web that is intentionally hidden, requiring access through a specific browser.

Wikipedia claims that the dark web contains 500 times more information than the indexed web. That may be true but since it's hidden, it's hard to make that kind of estimate. To cut the fantasies short, remember this: the dark web is just what is not indexed by Google. Most of the content on Facebook is not. The deep web is financial information, shopping catalogues, flight schedules, medical research and all sorts of things stored in databases that remain completely unnoticed by search engines. Portal content is often not indexed. This does not mean that the information is not accessible because it is that said, the dark web is still between 60 and 70% illegal activity, at least according to a 2016 study by the University of Surey.

For amateurs, ransomware kits have been available on the dark web for several years, and these offers have become much more dangerous with the rise of specialized criminal groups who develop their own malware, sometimes combined with pre-existing tools, and distribute them through "affiliates".

These attacks often involve stealing the victims' data and threatening to release it if the ransom is not paid. The difference between this method and the emails I receive every week, informing me that totally naked pictures of mine will be released if I don't pay soon, is that with the tools bought on the dark web, we are no longer at the stage of a simple threat spammed millions of times, but a targeted and equipped attack. We are in the virtual crime industry, and since they are covered by the multiple protections offered by the dark web, they are not about to get caught.

You've just installed Tor and you're already salivating. You see a nice search bar and think to yourself, this is much easier than you thought. You start typing in obscure words in the hopes of hitting some crazy sites, and you find that everything you find, you would have found with Google because until then, you've just been using DuckDuckGo, the search engine built into Tor. All you have so far is anonymous surfing. All dark web sites end in .onion. No .fr, no .com, just .onion.

So does that mean Tor is useless except for discreet surfing? What a disappointment! Rest assured dear 007 of the net, that's not the case at all. While Tor doesn't give you access to the dark web, it's a must-have if you

want to go there. When you have found an address.onion, run it through the Tor search engine and you're off on a journey to the land of the dark web.

There isn't really a dark web search engine like Google. We're in a world of anonymity, did you expect hollogram ads? The dark web was never meant to be organized or indexed.

Of course there are ways to find lists of sites but don't overlook the fact that they can disappear between one day and the next.

Why is the Deep Web not indexable?

There are several methods that prevent web pages from being indexed by traditional search engines. I have categorized them for your reference below:

- **Contextual Web** : Pages with content varying for different access contexts.
- **Dynamic content:** Dynamic pages which are returned in response to a submitted query or accessed only through a form, especially if open-domain input elements are used; such fields are hard to navigate without domain knowledge.
- **Limited access content** : Sites that limit access to their pages in a technical way (e.g., using the Robots Exclusion Standard or CAPTCHAs, or no-store directive which prohibit search engines from browsing them and creating cached copies).
- **Non-HTML/text content** : Textual content encoded in multimedia (image or video) files or specific file formats not handled by search engines.
- **Private Web** : Sites that require registration and login (password-protected resources).
- **Scripted content** : Pages that are only accessible through links produced by JavaScript as well as content dynamically downloaded from Web servers via Flash or Ajax solutions.
- **Software:** Certain content is intentionally hidden from the regular Internet, accessible only with special software, such as Tor, I2P, or other darknet software. For example, Tor allows users to access

websites using the .onion server address anonymously, hiding their IP address.

- **Unlinked content:** Pages which are not linked to by other pages, which may prevent Web crawling programs from accessing the content. This content is referred to as pages without backlinks (also known as inlinks). Also, search engines do not always detect all backlinks from searched web pages.
- **Web archives:** Web archival services such as the Wayback Machine enable users to see archived versions of web pages across time, including websites which have become inaccessible, and are not indexed by search engines such as Google.

What does the Deep Web Contain?

I have listed below some of the rare things found in the hidden dark world. These are:

- Mail Order Marijuana
- Silk Road
- Hitman Service
- Buttery Bootlegging
- The Human Experiment
- Weapons
- Credit Card Information
- Betting on Fixed Sporting Events
- The Hidden Wiki
- Recent Developments

How to find onion sites?

As a reminder, you can only access them through the Tor search engine.

Hidden Wikki is a "dark web" version of Wikipedia where you can find links to various sites on the dark web. As you can see, many of the onion links look nonsensical, as they are made up of a combination of many random numbers and letters. This makes it difficult to find the website you are looking for. Hidden Wikki does much of the searching for you.

However, as a caution be careful not to click on a link to something you don't want to see, because Hidden Wikki doesn't just index legal websites. In

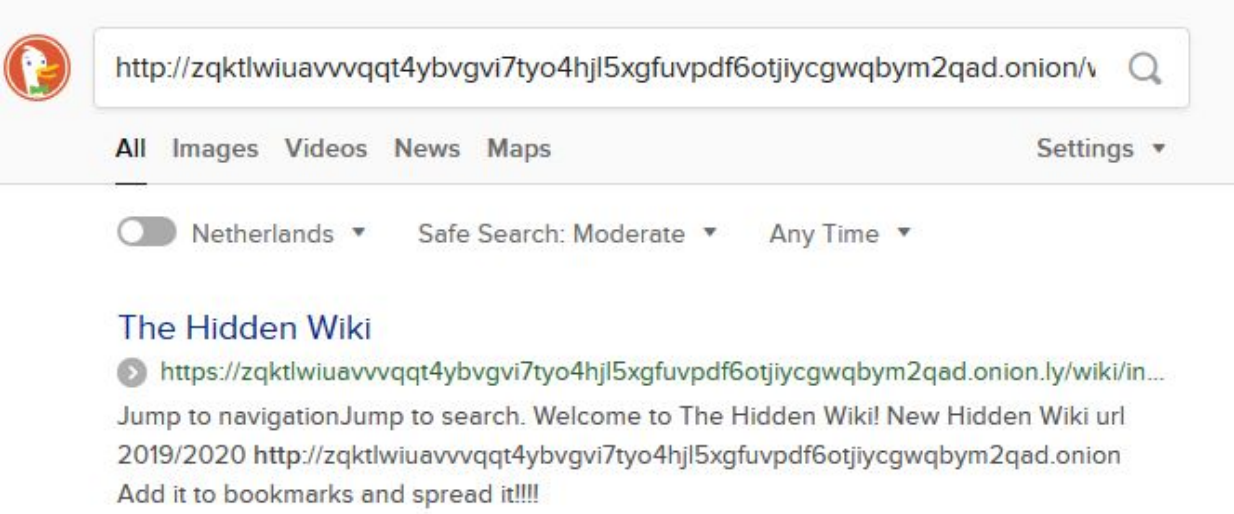
fact, there are many different "Hidden Wiki" sites. The Hidden Wiki was known to host, or at least index, a number of paedophile websites and has therefore been the subject of cyber-attacks by the FBI and Anonymous. Many imitators and derivatives of the Wiki have also been created.

Don't be surprised if you come across several versions of "The Official" or "The Uncensored" Hidden Wiki. If you type "Hidden Wiki" into Tor, this is what will happen.

This is the address of the original site:

http://zqktlwiuavvvqqt4ybvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbym2qad.onion/wiki/index.php/Main_Page

If you only have the paper version of this book, it will be complicated. Remember to only run the address through Tor. If you try it with Google anyway, it won't work.



Here are a few more, the sites disappear very quickly, so if it doesn't work, don't send me a scathing email, just move on to the next one:

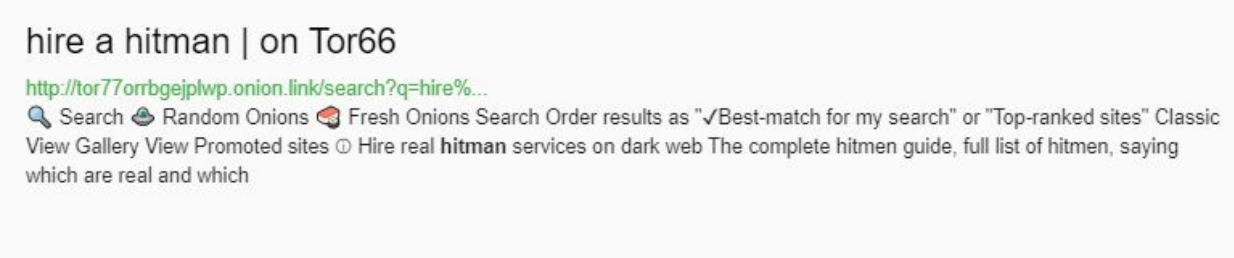
http://3g2upl4pq6kufc4m.onion
http://visitorfi5kl7q7i.onion
http://msydqstlz2kzerdg.onion
http://xmh57jrzrnw6insl.onion
http://7pwy57iklvt6lyhe.onion
http://bznjtqphs2lp4xdd.onion

http://searchb5a7tmimez.onion
http://gjobqjj7wyczbqie.onion
http://kbhpodhnfxl3clb4.onion
http://carontevaha5x626.onion
http://ulrn6sryqaifefld.onion/
http://onionlinksv3zit3.onion
http://hiddenwikiwpn2ed.onion
http://wikikijoy3lk2anu.onion
http://thedarkwebpugv5m.onion

None of these links are strictly speaking a search engine. They are more like lists of links. If you want to find more, you can use Google with phrases like "onion links", "Dark web links" or "dark web onion". You will find thousands of links that you can use via Tor. Before you venture out into the field, know that you are safe going through Tor.

Remember you're not safe once you're on the ground, because once you exit Tor and are on a Dark Web site, your IP address becomes visible and identifiable. You will need a good antivirus and a VPN. You will find that your browsing is slowed down. This is normal. Each of your requests is sent to a server, which sends it back to another, which ensures your anonymity.

Finally, if you are looking for the collaboration of a hacker, this is where you will find it. Just type "hack" or "spy" on Tor, and you'll immediately be put in touch with hundreds of providers from all over the world.



Just to show you how easy the dark web is, above you find a site that not only allows you to find a professional killer, but also gives information on the performance level of the person in question. I have no idea if this site is serious or not, that's not what's important. What I wanted to show you is that if you want something, the dark web has it.

https://darksearch.io/ wants to be the first search engine for the dark web. Nice ambition, interesting but offers so many broken links that it can be

annoying. There are secure markets on the Darkweb. These are markets in the original sense of the term, i.e. they host sellers who are registered on the site. This is a relative guarantee that you won't be cheated. Each marketplace has its own security rules for purchases, but also about what can be found there. Some marketplaces refuse the sale of weapons, drugs or child pornography, others are content to run the business without restrictions. Each seller, like any other e-commerce site, receives feedback from customers. As there are sometimes very bad comments, it inspires confidence but I personally haven't bought anything yet.

Another advantage is that these marketplaces have more sales than the sites that sell solo. I did a test two times in a two months period, and the marketplaces I had been to the first time were still active a month later.

Aurora Market

Adress: :
aurora7t7en7racqbytspft6myxds25hnczjk56tvqev2bziir74t4yd.onion

Aurora Market sells everything from drugs, fake documents, cracked/pirated/stolen digital goods, fraud-related items and a lot more. Over 12,000 products listed for now.

DarkFox Market

Address:
p5eg3xsssjglu6tvwfazp2nqqwfpah55wr3ljil2bezp5shix5ruqsqd.onion
On Dark Fox, we are totally uninhibited. Practically everything for sale is illegal. Drugs and medicines, counterfeit items, services (such as hacking/carding etc.), digital products (illegal software, hacked accounts etc.) fraud documents etc.

An excellent site to follow the particularly fluctuating news of the Darkweb: https://www.darknetstats.com

Finally, if you want to shop on the Darkweb, you'll have to be able to pay in bitcoins. Admittedly, the Darkweb is a mine for anyone active in intelligence though at your own risk.

XII. Organizing stakeouts and shadowing

I think the two most thankless activities for an investigator are stakeouts and tailing. I remember my last stakeout very well, it was on a Valentine's Day evening and I was taped to a lamppost waiting for someone to come and visit my target. The lights went out a little before midnight, I waited for another hour in the cold, and I went home where my girlfriend was not.

You go into intelligence, whether private or state, because you've seen a lot of movies and dream of living like your heroes. I wasn't disappointed with the job, it gave me what I expected and more but following someone is boring and stressful. A stakeout is boring and stressful. Surveillance and stakeouts are the two activities you do when you have no other choice.

I know it sounds stupid, but the influence of cinema is profound in these two activities. If cinema filmed reality, no one would go to the movies. Who wants to see a detective being run over at a red light or dying to pee when he's been watching the same door for ten hours?

Let's see how we can organize this.

1. Spinning

We will look at the different steps to organize your surveillance in the best possible way, as well as the situations to consider. Before you put your plan into action, remember that following someone may be harassment.

a)Planning

Never embark on a sting without first doing your homework. The more you know about your target's habits and actions, the more likely you are to follow them. You can't expect to follow someone without preparation.

Before you start, you should be able to answer the following questions about your target:

- Home address and place of work
- Time schedule
- Vehicle and registration
- Habits
- And, of course, their appearance

Many questions can be answered through social networks. Whether you need to tail the target from home or work, use a mapping tool to study the area and determine the routes your suspect might take and also identify shortcuts and wrong ways.

If your surveillance starts from a company, you need to know the different exits and identify which one is most often taken by the target.

As you will probably not be able to work alone, you will need walkie-talkies or spy micro-transmitters, which for this kind of job are much better than a mobile phone as you don't waste time forming a number and the communication doesn't break down in tunnels. Remember to buy some serious equipment, not the gadget you gave the kids for Christmas.

If you start the surveillance by car, put a tracker on the target's vehicle. This won't exempt you from a tail, as you never know when they will get out of the car, but it will take some of the stress off.

During this stage you check that your equipment is working and that you are not going to run out of gas.

b)Appearance

In real life, James Bond could not have been a field investigator. His character represents exactly what an investigator should never be.

- Always wear clothes that do not stand out or attract attention. The ideal look will be that of the place where you are going to work. If you start a walking tour in a business district, you will look like an executive. If it starts in a bad neighbourhood, you will look like a slob that goes with the walls of the area.
- If you are very good looking or very ugly, it is a big disadvantage because you will stand out. Also if you are of any ethnic minority in a place where there are few.
- **No** sunglasses, unless it's summer and other people are wearing them in the immediate area.

We recognize people not by details but by peripherals. If you are used to being around a person in uniform, the first time you see that person dressed in civilian clothes, it may take a while before you recognise them. The

peripherals of identification are the gait, general appearance, glasses, hat, bag, clothes, hairstyle, and general shape of the face.

You can be almost invisible to your target by regularly changing your peripherals. One moment you are wearing a cap, the next you are not. You have a reversible jacket that is blue on one side and green on the other. Neutral glasses one moment, no glasses the next. Same with all the peripherals. Including gait, which is a very big peripheral identification factor? I don't recommend make-up or a wig unless you work with real professionals.

Your client has probably given you information about the target. Preparation also means a good briefing. Because your client will often not give you all the information, either by negligence, by forgetfulness, by mistrust or sometimes just to test you. A bad briefing will make you lose a lot of time.

c)Surveillance

Most often, you follow a target who is travelling by car or on foot. In addition there are also motorbikes, bicycles, and public transport (bus, metro, train, plane) that you could use.

2. The car

Following a target on a motorway is not very complicated. Unless you are a moron, you keep a good distance from the target, and everything should be fine. You know the target is in the car now, you just don't know when he's going to get out of the car. That’s where the difference with a film starts. You need at least two people for a car chase. The driver and the "pedestrian", the one who will leave the car at the same time as the target. In a movie, the hero finds a parking space in a second. In real life, by the time you find one, the target is already far away. The "pedestrian" is used to avoid this. In the city, without a tracker on the target vehicle, a tail with one car is almost impossible. It's dead at the first red light. Any event makes you lose the target in 30 seconds. That's why a professional tailing is done with 3 vehicles and constant radio communication. Your vehicle follows the target, a second one follows the same axis on a parallel lane to your left, while the third one does the same to your right. As soon as the target changes direction, another vehicle takes over and the movement pattern

resets. Isn't that nice? 3 cars, minimum 6 people involved in the operation. Only the state services can afford this. A private person will rarely be able to convince a client to pay what is needed. This is because the client has also seen Starsky and Hutch. If you have an accident or your licence is revoked, the client will disown the deal.

Before you start, make sure you have a full tank of gas, snacks and any supplies you might need. If you are using equipment, such as binoculars or video cameras, have extra battery backup and test the equipment before you leave.

If you are outside a major city, you are much less likely to lose your target, but you do increase your chances of being spotted. The James Bond car, you forget, although I know of one detective who worked with a yellow Mercedes. Your car should be a very ordinary one. If your target has no reason to be suspicious, you have a chance. If they are a bit wary, an out-of-town tail with a single vehicle is highly unlikely.

On a motorbike

In the city, a motorbike is an excellent way to follow a target. You can weave in and out of traffic and remain almost invisible to the target by staying in their blind spot. If the target suddenly changes transport, it is easier to park a motorbike than a car. If you also have a colleague in the back seat, it's even better because your partner continues to follow on foot while you remain mobile and ready to take over the job, but it is very dangerous and the risk of accidents is very high. Riding a motorbike in normal circumstances is already an exercise that requires your full attention.

Paying attention to the environment and your target is only possible if you have a lot of experience on a motorbike.

Outside the city, the motorbike is not an advantage because you will be spotted very quickly, even if only by the beam of your headlight.

On foot

When following someone in public space, you never look at the target. I think this is the biggest mistake amateurs make. If your eyes meet the target's, that's it, you're done. You keep the target in your field of vision but

look to the left or right of it. Your pace is that of the street for if you start running you become identified, same if you walk too fast. Common sense is your friend. You can't follow your target everywhere. If, for example, she walks into a department store and wanders into the underwear department, you don't go there.

Use the shop windows to see without being seen. A guy alone will be spotted faster than a woman alone. A couple is even better. A dog is very good. I did a lot of tailing with my son when he was little. Who's going to think that a guy walking around with his kid is an investigator? Come on, a little glamour anyway. If you work in a team, which is a very strong suggestion, you need to communicate with each other quickly, accurately and understandably. Not at all the way you usually talk to your friends. Saying that the target is turning right doesn't mean anything. The right of whom? To where? It is clearer to say "The target is heading towards the Summer Breeze shop. I repeat, Summer Breeze. Over!" Your colleague must repeat the information to confirm it. This is secure communication and if you want to communicate like a pro on the phone or with a walkie-talkie, this is a must. The target has a code name. So does every member of the team. Not to look pretty, but because it's practical. On the phone, the sounds don't come through that well. There is often confusion.

A-Alpha B-Bravo C-Charlie
D-Delta E-Echo F-Foxtrot
G-Golf H-Hotel I-India
J-Juliett K-Kilo L--Lima
M-Mike N-November O-Oscar
P-Papa Q-Quebec R--Romeo
S-Sierra T-Tango U--Uniform
V-Victor W-Whiskey X--X-ray
Y-Yankee Z-Zulu

The above is Nato's phonetic alaphabet. But everything related to security uses it. Police, fire brigade, armed forces, civil protection etc. It is a simple and effective way of avoiding blunders due to misunderstandings. Learn it by heart, you'll get the hang of it very quickly. And if you never use it during a mission, you will find a way to show it off.

If your target has a regular schedule, one technique that allows the agent to avoid detection is to segment the mission over several days. On the first day, you follow the target over a shorter or longer distance. On the second day, you resume the tracking from the previous day's stopping point. This is a technique used by the police or intelligence services when, for example, the target's home needs to be identified.

3. The stakeout

Stakeouts differ from shadowing in that they are used for static observation. It can be practiced in urban or non-urban environments, and we will see that this is quite different. But whatever the location, you don't know how long it will last. So take something to eat and drink. You never know how long a surveillance will last. Often long hours without being able to move. If you are in the private sector, you will be lucky if the client agrees to pay two investigators, so often, for a simple static surveillance, you will be alone and so, think of a technicality: if you have a health emergency, what do you do? Do you leave the surveillance for a few minutes at the risk of compromising the mission? Do you carry nappies? Or do you carry an empty bottle to relieve yourself? If you are a woman, you will have to be creative.

In an urban environment

Normally crowds or traffic will protect you. If you are in a car, try to park so that you can observe via your rear-view mirror, it's much more discreet. It's very hard because your attention can't drop for a second. A second is the time it takes for a door to open or a bus to pass. Here again we have a nice difference with the movies: telling your life story to your partner while drinking is nice, but it's not reality. Here you observe and that's it, for a long time.

If you're lucky enough to be able to hide out in a bar, that's fine. Nobody will ask you anything as long as you drink. NB you ought to pay for your drink when you get it, as it is not ideal to have to dig into your pockets when your target leaves his house, or worse, you have to wait for your change because you only have a 50 euro note. I'm not talking about the very cinematic case where you've rented the flat opposite your target to watch him, or her 24/7, for in reality, that doesn't exist in the private sector.

In rural or suburban areas

Stashing away in the countryside or in a housing estate is very complicated. If you stay in your car, you will be spotted. Unlike in the city, if you are spotted in the countryside or on a housing estate, someone will quickly ask you what you are doing there or call the police. You are not committing a crime, but the stakeout will be over.

If you have no other option, at least have a story to justify your presence as a real estate agent on the lookout, future resident of the neighborhood etc.

If the mission allows it, remote observation is a good option. If you are equipped with a powerful monocular with night vision, you can stay undercover for long hours, without missing anything about your target's activities. If you don't want to miss anything, and if you have a window of opportunity to install them, the use of spy cameras will be of great help. The best option here is the submarine, a vehicle disguised for intelligence purposes. A van with a plumber or electrician logo is fine. With a phone number that you answer if a neighbor checks. If you are lucky enough to be able to hide from the church square, you should be fine as long as the people around you can't identify that you are in the vehicle. If not, park in such a way as to make the locals think you are doing work on a neighbor’s house. Wear workman's or technician's clothes, with a cap, as this is exactly the profile that nobody pays attention to. Your outfit should not be too new nor too clean. If you don't know how long the job will last, bring changing clothes too. The weather is not your friend. If you are on surveillance in a car and it is cold, you will suffer because you cannot move. Also, it will fog up and make you noticed. If it is very hot, you cannot open the windows wide and your agony will be long.

Your job is often to take pictures through the windscreen or the rear-view mirror. If the glass elements are dirty, your photos will be of poor quality. It is therefore important that your vehicle is clean but if it rains, taking pictures through the windscreen will be almost impossible. Have a good night.

XIII. Managing your network of informants in a completely anonymous way

Now you have your network of informants. They work in ministries, banks or telecommunication companies. As you are not working against the interests of a country, you are in private intelligence, remember, the risk is low of finding yourself with a group of Mossad agents hidden in your garden. However, you are careful and I congratulate you for that.

You must have met the members of your network on several occasions, but for the sake of discretion, you want to be able to communicate with them anonymously. Above all, you want a safe way to receive their information. Before the Internet, you had to use two very dangerous means. The dead letter box or the physical exchange. The dead letter box is anything in the public space where an agent can leave a document or a message. A mark warns that the delivery has been made. This mark can be near the mailbox or in any part of the city. Signaling devices can include a chalk mark on a wall, a piece of chewing gum on a lamppost or a newspaper left on a park bench. The signal can also be emitted from inside the officer's home, for example by hanging a particular colored towel on a balcony or placing a potted plant on a windowsill where it is visible to everyone on the street. Although the direct delivery method is useful for preventing the instant capture of a couple of agents or an entire network, it is not foolproof.

If one of the agents is compromised, he or she may reveal the location and signal of that specific drop point. The police can then use the signal while keeping the location under surveillance, and can capture the other agents. Another disadvantage is that an operator will carry something on him for some time that can harm him. It will be the same when you come to collect the equipment. You have it with you. Finally, if your informant lives 800 km away, it is not very practical.

The exchange technique requires that two agents pass each other in a public space (street, shop, toilet, etc.) and that one gives something to the other. Apart from the stressful aspect, the disadvantages are the same as with the dead letter box.

That's why at the beginning of your mission, you simply created an account on a free mailbox. As you had to give an email address for the confirmation of the creation of the address, you took care to do it with a disposable email address. You installed a VPN so that your IP address cannot be traced, you never use Google because you know that everything is recorded and instead you work with Duckduckgo. You erase all traces on your machine with an excellent free tool, ccleaner https://www.ccleaner.com/ but you still take the paid option because it gives you a much nicer deep clean.

When your informants are recruited, ask them to memorize the email address and access code. Then give them these security instructions:

- Never use the office computer because everything is recorded on the box's server.
- Use a VPN and cleaner.
- Go online exclusively via duckduckgo.

Never use your name, nor the name of the operator. You can choose any name you want, but none that links you to it. In the old days I had an informant called 'Angelina'. Why? Because she was a look-alike of the American actress Angelina Jolie.

To pay your informant, it will be via an offshore account if we are talking about large amounts. If we are talking about sums of a few hundred or thousands of euros, you use a dead letter box system. This is not very dangerous because if you or he is caught, you have a ready-made story that justifies you being in possession of this sum. If its 100,000, euros don’t waste your time making up a story, you are caught!

Every time your informant wants to give you information, he logs on to the mailbox, writes his message with his code name in the header, with an attachment if necessary, and saves it in the drafts. No message is sent. No information flow. When you log on to the mailbox, you access the message and then delete it. The box is empty. You run cleaner.

Of course, there is always a risk if you have to download data. At the very least, do it by downloading to an encrypted USB stick. An even more discreet way to do this is to create an account on a gaming or dating site.

In any case a site where you can write a message and then save it without sending it. This is fine, but it is rare that it is possible to save attachments.

The risk here is mainly related to routine. You know that your life is not at stake. The offences committed will not send you 20 years behind bars. I've known people in private security who regularly go out for a meal with their sources and just before dessert they take out a little envelope. They got caught and spent a few weeks or months in jail. If you're really careful, that won't happen. But what is complicated is controlling the level of vigilance of your operators. Security is good, but it wastes time. Since nothing ever happens, we tend to relax. As is often the case, the human factor will be our undoing.

XIV. Conclusions

A few years ago I wrote a book with the unambiguous title "How to make your boss's life miserable". It was all about recipes for dirty tricks. Some of them were just plain funny. Others were so intense that they could ruin your boss's life. A lot of people asked me if I was worried that people with malicious intent might use the book's contents to harm their boss. Each time, I asked the same question: "Would you do it?" Each time, the person answered that he or she would not, but that others might. It is well known that the evil is the others. I wrote this book because I was tired of hearing people whining in companies. Whining about how the boss or manager had all the power and they had none. When you know that if you want to, you hold your boss's very existence in your hands, it's much harder to position yourself as a professional victim.

"Offensive Intelligence" can be seen in exactly the same way. A book about the power that any anonymous person has if they want it. You now know that privacy is a thing of the past, that you can get any information you want without being part of a state intelligence agency, and that if you want to, you can do great harm to any company. Although there is no chapter explicitly devoted to destroying anything, a careful reading of many chapters gives you the power of a weapon of mass destruction. The Truth, I hope that no one will be harmed and that everyone can find what they are looking for.

On another level, this book is all about safety. Nobody likes to take the place of the victim. That is why books about security are not really massively successful. In this case you are in the shoes of the attacker. It's much more fun and just as instructive. When you see what you can do with very little, you can start thinking about how to protect yourself.

Finally, the real purpose of this book is neither security nor an ode to power. It is a practical manual that aims to teach you how to obtain intelligence on companies and decision-makers. The rest is secondary in my eyes.

I suggest you work with both the paper and electronic versions. There are a lot of clickable links and with the paper version you will have to manually retype the links and that is rather annoying to do.

In anticipation of mea culpa for the dead links you'll probably run into I have this to say “We die young on the net and a lot of things disappear very quickly”. If you come across an error, an inconsistency or a dead link, let me know and I can keep this manual updated. The same goes for any technique or tool that you know of that should be known to everyone.

To contact me use the email address,

dylewskiphilippe@gmail.com

If you want the EBook version for free, you can also reach me at this address. The electronic version is mostly useful for clicking on the links.