Philippe Dylewski

LE RENSEIGNEMENT OFFENSIF

300 techniques, outils et astuces pour tout savoir sur tout le monde, dans les entreprises et ailleurs

Deuxième édition mise à jour 2021

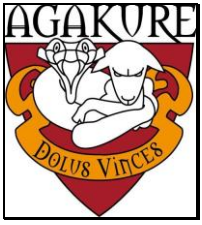


Table des matières

9. Investigations poussées via les images satellite
10. Traquer une cible en lui envoyant un lien de détection

IV. Les techniques et outils de Sourcing de candidats
1. Trouver des emails de candidats sur LinkedIn
2. Automatiser la recherche sur LinkedIn ? Les limites de LinkedIn et comment les contourner
3. Trouver des emails de personnes travaillant dans l'entreprise que vous ciblez
4. Trouver des candidats sur LinkedIn en passant par Google
5. Rechercher des candidats sur LinkedIn avec un compte gratuit

V. Le matériel d'espionnage
1. Espionner un téléphone à distance
2. Le stylo espion
3. Le drone avec caméra
4. La balise GPS pour filature à distance
5. Regarder sous la porte. L'endoscope
6. Ecouter à travers la porte ou le mur. Le stéthoscope
7. Voir sans être vu : la mini caméra espion
8. L'observation discrète en milieu urbain : le monoculaire
9. Brouiller le signal d'un téléphone portable/d'un réseau WIFI ou d'un signal GPS
10. Détecter les micros dans mon bureau
11. L'amplificateur de sons
12. L'enregistreur de frappes clavier
13. Le micro espion
14. Le VPN
15. Clonage d'un disque dur ou d'un téléphone

16. Outils de cryptographie
17. Téléphone jetable anonyme
18. Un lecteur de carte SIM pour lire les SMS d'un téléphone éteint
19. L'écoute d'un portable à distance. L'IMSI catcher
20. La carte de crédit anonyme

VI. Débusquer les mensonges d'un CV

VII. Tout savoir sur vos concurrents

1. Le renseignement humain pour tout savoir de ses concurrents et (futurs) partenaires
2. Détecter le mensonge
3. Comment inspirer confiance à sa cible
4. La manipulation au service du renseignement offensif
5. Usurper une adresse email ou envoyer un email anonyme
6. Faire les poubelles
7. Contacter les clients de la concurrence
8. Les foires et salons
9. La corruption
10. Surveiller les brevets de la concurrence
11. Tracer les modifications d'un site
12. S'abonner à la newsletter de votre concurrent
13. Tout savoir de la stratégie en ligne de votre concurrent
14. Les groupes de discussions
15. Les blogs
16. Les archives des journaux et revues
17. Identifier les clients du concurrent
18. Identifier les fournisseurs du concurrent

I. Introduction

La première édition de ce livre date de 2010. A la base, ça ne devait pas être un livre mais un manuel que je créais petit à petit pour m'aider dans mon boulot de détective privé. La charmante madame avec qui je vivais à l'époque m'a amoureusement signalé que si les romans d'espionnage pullulaient, il n'en était pas de même des manuels d'espionnage.

J'ai fait une mise en page approximative, et fait imprimer 100 exemplaires au copy service du coin de la rue. Tout a été vendu en une semaine. Quelques mois plus tard, lassé de timbrer et de mettre sous enveloppe, j'ai voulu tenter ma chance auprès d'éditeurs. Comme je n'en connaissais aucun, j'ai utilisé un robot collecteur d'adresses que j'ai lancé à l'assaut de Google. A la fin de la journée, j'avais plus de 5000 adresses Email d'éditeurs francophones. La précision des adresses n'était pas top, puisque j'avais des adresses d'éditeurs de manga, de livres pour enfants ou d'ouvrages consacrés au terroir. J'ai utilisé une plateforme d'envois de mails et en une heure, tout était parti avec une jolie lettre et le sommaire du bouquin.

Au bout de quelques semaines, j'avais reçu six propositions de contrat et j'ai signé avec l'Express. Rien à dire, ils ont fait le boulot. Ils ont fabriqué un beau livre, en ont fait la promotion et j'ai connu le bonheur narcissique d'aller me balader dans les librairies afin de savoir s'ils avaient mon bouquin en stock. Le seul inconvénient, c'est que le livre traitait d'un sujet sensible et que pour des raisons juridiques, il a fallu sabrer dedans. A l'époque, ça m'avait semblé normal qu'un éditeur veuille se protéger

d'éventuelles poursuites. Je n'ai d'ailleurs pas changé d'avis. Mais si je voulais écrire un livre vraiment offensif, il fallait que je me sente libre d'écrire ce que je veux, y compris le pire. C'est ce que vous commencez à lire.

Ce livre s'adresse aux professionnels :

- Détectives privés, spécialistes de la veille et de l'intelligence stratégique.
- Journalistes.
- Responsables marketing.
- Dirigeants de PME.
- Recruteurs.
- Cabinets d'avocats.

Il ne s'adresse pas aux responsables de la sécurité informatique ni aux gourous du marketing digital. D'une part parce qu'ils n'apprendront pas grand-chose dans leur secteur, et d'autre part parce que ce bouquin se place délibérément dans la peau de l'attaquant. Il n'a pas pour ambition de protéger votre réseau informatique ni de vous aider à vendre sur Amazon.

L'objectif est simple : fournir des outils, des techniques et méthodes qui vous donnent accès à des informations sur vos concurrents, fournisseurs, clients, collaborateurs et partenaires commerciaux. Dans ce que je vois au quotidien, mes clients prennent souvent des décisions importantes sur base de bien peu de choses. Un bon bilan, un beau CV, un peu de sympathie, et l'instinct fait le reste. Un beau bilan ne

signifie rien, un beau CV peut être bidon, et votre instinct vous a trompé des tas de fois depuis que vous êtes né.

J'ai souvent entendu des dirigeants dire des trucs du genre « ce que fait mon concurrent, je m'en fous, je ne regarde pas ce que fait le voisin ». L'attitude est sans doute noble, mais elle ne me semble pas différente de celle de l'officier qui envoie ses hommes au combat sans rien connaître de l'ennemi.

En aucun cas je ne conseille d'espionner un concurrent dans le but de le copier. Seulement pour faire mieux. Pour ne pas être largué. Surveiller vos concurrents, c'est apprendre de leurs forces et de leurs faiblesses, ce qui fonctionne et ce qui ne fonctionne pas. Il s'agit d'apprendre et de grandir.

Ce manuel que vous tenez entre vos mains tremblantes d'émotion se veut d'utilisation simple. Il vous sera proposé des centaines de trucs, de méthodes, d'outils et de liens. Sont exclus de ce livre, tout ce qui a trait à la programmation et tout ce qui suppose des prérequis techniques de niveau élevé. Les outils coûteux en sont aussi absents. Cependant, il s'agit d'un manuel. Le lire ne sera pas suffisant. Si vous voulez donner du sens à l'achat de ce livre, il vous faudra travailler et vous entrainer. Sans ça, ce sera inutile.

II. Recherches approfondies sur Google et Google hacking

1. Les moteurs de recherche

La base du renseignement à distance, c'est Google. Incontournable. D'ailleurs, vous l'utilisez déjà. Google est à ce jour le moteur de recherche numéro 1 au monde.

Il présente cependant un inconvénient majeur : celui de traquer vos activités pour son compte ou le compte de tiers. Bien entendu, vous n'avez rien à cacher. Ce qui vous amène peu fréquemment à vous balader tout nu devant votre fenêtre. C'est bien connu, si nous n'avons rien à cacher, cela ne veut pas dire que nous sommes d'accord de tout montrer.

N'oubliez pas que vous utilisez ce manuel à des fins d'espionnage et que vous serez peut-être amené à faire des requêtes qui pourraient un jour avoir des conséquences fâcheuses. Heureusement, il vous sera expliqué plus loin comment anonymiser vos recherches.

Google n'est pas uniformément présent dans le monde entier. La Chine ou la Russie ont leur propre moteur de recherche alternatif et si vous avez des investigations à mener dans ces zones, il sera indispensable de les utiliser. Nous allons très vite voir comment surmonter la barrière de la langue.

Baidu est le premier moteur de recherche en Chine, avec une part de plus de 70% du marché Internet chinois. Les

statistiques divergent à ce sujet. Il a sensiblement le même design que Google. Si votre enquête se porte sur la Chine, pas le choix. Attention que ce moteur est très censuré et si votre recherche a des connotations politiques, il y a de grandes chances que vous ne trouviez pas votre bonheur. Ce moteur ne présente d'intérêt que si vous pouvez faire des requêtes en chinois.

https://www.baidu.com

Je ne résiste pas au plaisir de vous montrer que j'ai un bouquin traduit en chinois. Si je fais la même recherche sur Google, je ne trouve pas ce lien. Ci-dessus, la recherche est menée dans notre alphabet alors que je viens d'écrire qu'une requête sur Baidu se doit d'être rédigée en chinois. Le cas est particulier : le livre traduit en chinois a une couverture en chinois, mais le nom de l'auteur est écrit dans les deux alphabets.

Yandex est un moteur de recherche très utilisé en Russie, où il est leader du marché. https://yandex.ru/ est en russe exclusivement mais autorise les recherches en anglais ou en français. Ce qui ne vous avancera pas à grand-chose car si vous recherchez une information spécifiquement russe, vous ne l'obtiendrez qu'en la demandant en russe. Nous

verrons plus loin qu'il existe un traducteur intelligent qui va régler de façon définitive votre ignorance du chinois et du russe.

Il existe des tas d'autres moteurs de recherche. Les plus connus sont Bing, Yahoo ou Ask. D'autres sont moins connus et offrent une garantie de discrétion. Il y en a même qui sont écologiques, en tout cas d'après leurs dirigeants.

Bing a réellement un point fort par rapport à Google : sa cartographie est d'un meilleur niveau et sa recherche de vidéos est plus conviviale. A part ça, Google reste le maitre du monde.

2. La recherche de base

Google n'a accès qu'à moins de 10% du web total, 90% du reste appartenant au web invisible. C'est ce qu'on dit. On a toujours dit la meme chose avec le cerveau humain dont nous n'utiliserions qu'une faible partie du potentiel. Ce qui est certain, c'est que l'information est tellement abondante, que si vous ne disposez pas d'outils de tri ou de recherche approfondie, vous ne trouverez pas exactement ce que vous cherchez. Google utilise un système de classement appelé PageRank pour classer les résultats d'une recherche du site le plus pertinent au moins pertinent. En fait, plus l'adresse d'un site est répertoriée par d'autres sites, plus ce site est pertinent : chaque lien pointant vers une page est considéré comme un vote pour cette page. Ce qui veut dire qu'en menant des requêtes classiques, vous tombez sur les résultats les plus populaires, pas forcément les plus pertinents.

C’est pourquoi vous allez devenir des pros de la recherche booléenne. La recherche booléenne est une méthode d'interrogation qui permet d'élargir, de restreindre ou d'affiner les résultats de la recherche. Dans le domaine du recrutement, la recherche booléenne permet de localiser rapidement et efficacement les candidats idéaux pour les postes vacants. Semblable à une fonction de "recherche avancée", les opérateurs de recherche booléens vous permettent d'inclure, d'exclure et de baliser des mots clés spécifiques pour affiner soigneusement vos résultats de recherche. En fin de compte, l'utilisation de la recherche booléenne dans le domaine du recrutement a pour but d'affiner les thèmes généraux - tels que les titres de poste ou les exigences - afin d'identifier un vivier de candidats.

Tout ce qui suit vous sera surtout indispensable quand vous recherchez quelque chose de pointu et qui nécessite d’être trié. Si vous cherchez une ancienne copine dont le nom et le prénom sont assez originaux, ne vous cassez pas trop la tête avec ce qui suit. Mais si vous cherchez Alain Delon, électricien dans le sud de la France, ou les probables liens entre votre cible et une entreprise, lisez attentivement la suite.

Les guillemets

C’est le tout premier truc à connaître lorsque l’on se lance dans des recherches sur Google. Une règle de base qu’il est primordial de répéter à chaque fois que vous recherchez une expression bien précise. Les guillemets vous permettent en effet de rechercher une suite de mots ou de noms dans un ordre très précis. Ainsi, si vous tapez "marketing manager

bruxelles", vous trouverez uniquement les liens vers ces 3 mots précis. La même requête sans les guillemets peut vous mener sur des pages très différentes ou il sera bien question de marketing mais où les termes « manager » ou « Bruxelles » peuvent apparaître pour n'importe quelle raison.

Les guillemets sont évidemment d'usage pour rechercher des informations sur une personne ou une adresse : "prénom nom", "adresse code postal ville". C'était surtout vrai il y a quelques années. Aujourd'hui, si vous tapez « philippe dylewski » ou philippe dylewski, les premiers résultats seront les mêmes. Mais quand une requête devient complexe, les « » deviennent indispensables.

Si je fais la même requête sans les « », les premiers résultats sont quasi identiques. La différence, c'est qu'au lieu de recevoir 28 résultats, j'en reçois plus de 7.000.000. car très rapidement, je reçois des liens vers des pages comprenant le mot « marketing » ou « manager » ou « bruxelles ».

Pages en cache

Lorsque Google explore le Web, il crée une copie de chaque page examinée et la stocke dans une mémoire cache, ce qui permet de consulter cette copie à tout moment, et en particulier dans le cas où la page originale serait inaccessible. Lorsque vous cliquez sur le lien « en cache » d'une page Web, Google affiche celle-ci dans l'état où elle se trouvait lors de son indexation la plus récente. Par ailleurs, le contenu caché est celui sur lequel se base Google pour déterminer si une page est pertinente pour vos requêtes.

Lorsqu'une page cachée est affichée, elle est précédée d'un en-tête encadré qui rappelle qu'il s'agit de la copie cachée de la page et non de la page originale, et qui cite les termes de la requête ayant entraîné son inclusion dans les résultats de recherche. Pour faciliter l'exploitation de cette page, les différentes occurrences des termes de recherche sont également surlignées dans des couleurs différentes.

Le lien « en cache » n'apparaît pas si le site n'a pas encore été indexé ou si le propriétaire du site a demandé que le contenu caché soit exclu de l'indexation Google.

Tout ça n’a réellement d’intérêt que si la page a disparu du web. Ce qui arrive très souvent. Ou aussi si vous voulez aspirer des adresses email à partir d’un document PDF. En

effet, la plupart des robots collecteurs d'adresses ne parviennent pas à aspirer des données à partir d'un fichier PDF. Mais si vous parvenez à ouvrir le document avec le mode « en cache », l'aspirateur fonctionnera. Donc, fonction très utile.

Ponctuation & majuscules

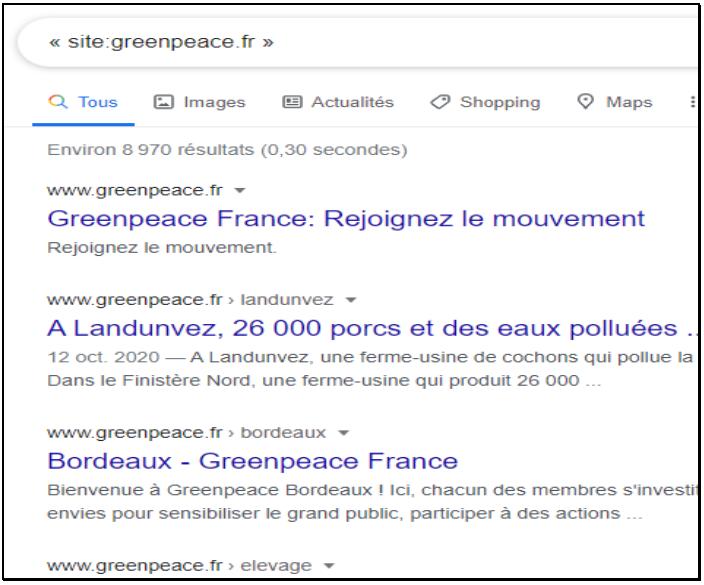
Majuscule ou minuscule, Google ne fait aucune différence. Pas la peine de se casser la tête. Idem pour la ponctuation, les tirets et autres cédilles. Laissez tomber, Google ne les voit pas. Même le signe arobase (@) n'est pas reconnu, ce qui est un peu ennuyeux quand je fais une recherche d'adresse mail. Attention que cela n'est pas forcément vrai pour d'autres moteurs de recherche. Par exemple, Duckduckgo reconnait le signe (@), ce qui peut avoir son intérêt pour certaines recherches.

Restreindre une recherche à un site particulier

L'information recherchée se trouve sur un site en particulier. Si vous tapez l'URL du site (par exemple www.greenpeace.fr), vous accédez au site bien évidemment. Vous vous retrouvez sur la page d'accueil du site et vous pouvez commencer vos recherches dans un océan d'informations.

Si vous faites une requête Google « greenpeace.fr », vous allez obtenir des tas de liens qui parlent de Greenpeace. Alors que si vous utilisez le terme « site:greenpeace.fr », vous n'obtiendrez que les liens qui mènent vers le site de

Greenpeace France. N'oubliez pas de taper « site:greenpeace.fr » sans espace. Si vous laissez un espace, la formule ne fonctionne pas.



Jusque-là, le seul avantage est d'obtenir une vue générale du site à étudier. C'est pas mal, mais pas de quoi se mettre à danser la polka.

Mais si je veux faire une recherche précise dans un site, sur un thème ou un nom donné, c'est possible. Dans l'exemple suivant, je recherche les références à Nicolas Sarkozy sur le site de Greenpeace.fr et uniquement cela. Avec 431 résultats, je crois que nous pouvons dire que chez Greenpeace, on aime, ou on aimait, parler de Nicolas Sarkozy.

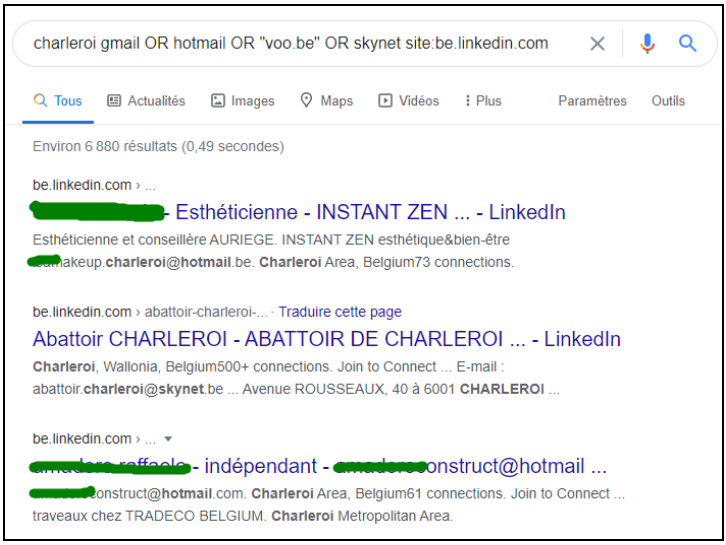
Cette astuce est intéressante lorsque vous menez une recherche sur un site de taille considérable. Utile quand l'info se trouve sur le site d'un journal ou d'une revue, même si vous pouvez obtenir le même résultat avec leurs archives.

Vous pouvez utiliser la fonction site : pour faire des recherches spécifiques sur le site de votre concurrent. Attention, rien que vous ne trouveriez en l'épluchant tranquillement. Vous gagnez du temps. Par exemple, si vous voulez connaître les tarifs de votre concurrent, vous tapez *site:monconcurrent.fr tarif*. Si le tarif ne se trouve pas sur le site, aucune formule magique ne va le dégoter.

L'un ou l'autre

« OR » utilisé entre deux mots ou expressions vous rapportera tous les liens reprenant l'un ou l'autre de ces mots ou expressions. Cela vous fait gagner du temps car plus besoin de mener plusieurs requêtes.

Dans l'exemple suivant, je cherche à obtenir l'adresse email d'habitants ou d'entreprises de la région de Charleroi ayant un profil LinkedIn.



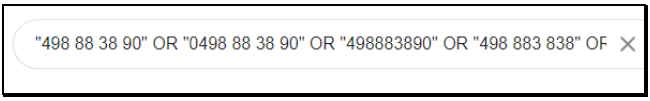
N'allez pas imaginer que j'ai découvert la formule secrète pour obtenir les emails sur Linkedin. Je ne trouve que ceux qui se trouvent sur le profil public des gens.

Cet opérateur est aussi utile quand vous n'êtes pas certain de l'orthographe de votre cible. Par exemple *dylewski OR dilewski OR dylevsky* vous ramènera tous les résultats sur base des différentes orthographes.

Toujours dans la recherche de personnes, cet opérateur vous permet de tester différentes variables de recherches en une seule requête.

« philippe dylewski » OR « dylewski philippe » OR philippedylewski OR pdylewski OR phdylewski

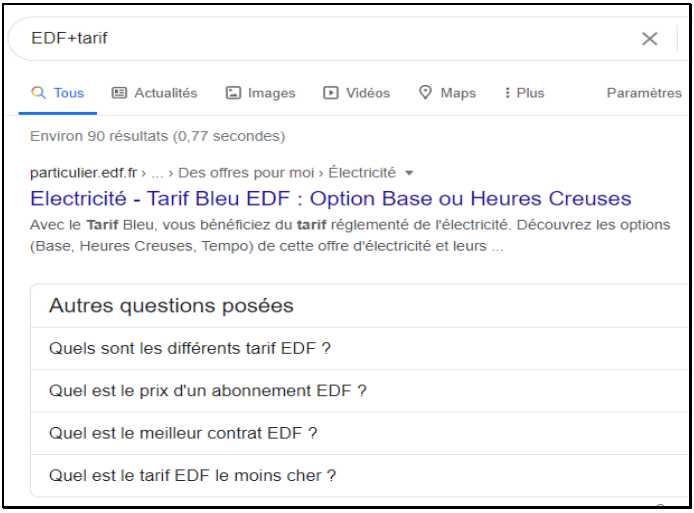
Enfin, quand vous ne disposez que d'un numéro de téléphone pour trouver de l'information sur une personne, la fonction OR est très utile puisqu'il existe différentes façons d'écrire ce numéro.



Ceci est le numéro de portable que j'utilisais jusqu'il y a peu et en deux minutes, on trouve mon adresse et un lien vers différents sites ainsi qu'un profil Facebook qui permet très rapidement de remonter jusqu'à moi.

L'un ET l'autre

L'opérateur « ET » n'a plus d'utilité aujourd'hui car quand votre requête est de plus d'un mot, le « ET » est d'application par défaut, ce qui n'était pas le cas dans le passé. Il y a quand même de petites différences, mais c'est mineur. Ce qui est intéressant dans l'exemple ci-dessous, c'est le pouvoir d'association de deux mots. Je veux connaître les tarifs EDF.



Recherche d'un mot clé dans l'url

Ce critère booléen permet de rechercher un mot-clé spécifique dans les URL d'une page web.

Exemple : *inurl :CV* permet de rechercher les pages web dont l'URL convient le mot CV.

Un autre exemple, pour trouver des caméras sans code de sécurité.

"Camera Live Image" inurl:"guestimage.html"

Trouver une carte

Maps : suivi d'un lieu vous permet de trouver immédiatement les cartes de cet endroit.

Tilde ~

Le symbole TILDE peut être utilisé soit pour élargir, soit pour réduire vos résultats de recherche. L'opérateur TILDE inclut dans les résultats des synonymes du mot-clé que vous marquez avec ce symbole.

Pour trouver le CV d'un vendeur, vous pourriez utiliser la chaîne de recherche suivante : *~CV "vendeur"*

Les résultats de recherche incluront tous les documents de type CV des profils de vendeurs. Si vous lancez votre requête telle quelle, vous allez avoir beaucoup de déchets. Vous allez surtout tomber sur des offres d'emploi, ou des modèles de CV ou encore des méthodes pour rédiger un CV qui vous garantissent le job de vos rêves. Pour éviter ça, vous pouvez combiner TILDE avec l'opérateur NOT :

~CV "vendeur" -modèle -exemple -emploi -méthode

Sur Google, cette chaîne de recherche vous permettra de générer des résultats contenant pour la plupart des CV réels de vendeurs. Vous pouvez également continuer à ajouter des opérateurs NOT pour réduire davantage les résultats indésirables.

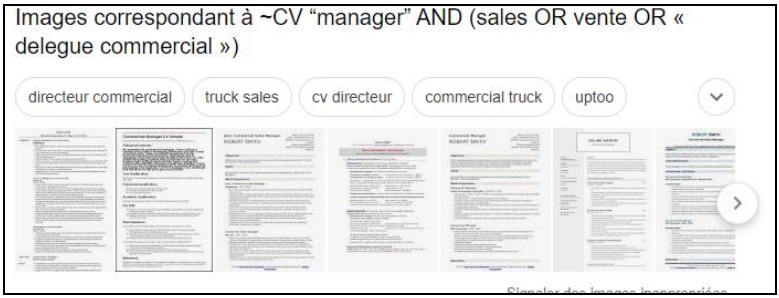
NEAR

NEAR vous permet de rechercher des mots (ou des expressions) qui apparaissent proches les uns des autres dans un document ou dans une page web. Il s'agit d'un opérateur de recherche de proximité qui recherchera

automatiquement les résultats contenant des expressions clés séparées par 1 à 10 mots dans le texte.

Par exemple, si vous recherchez le CV de managers commerciaux qui ont une expérience en vente, votre chaîne de recherche pourrait ressembler à ce qui suit :

~CV "manager" AND (sales OR vente OR « délégué commercial »)



Un p'tit oubli ?

Fonctionnalité : recherche de variations d'un mot racine. Utilisez l'opérateur astérisque pour élargir vos résultats de recherche lorsque vous savez qu'il existe de multiples variations d'un mot racine.

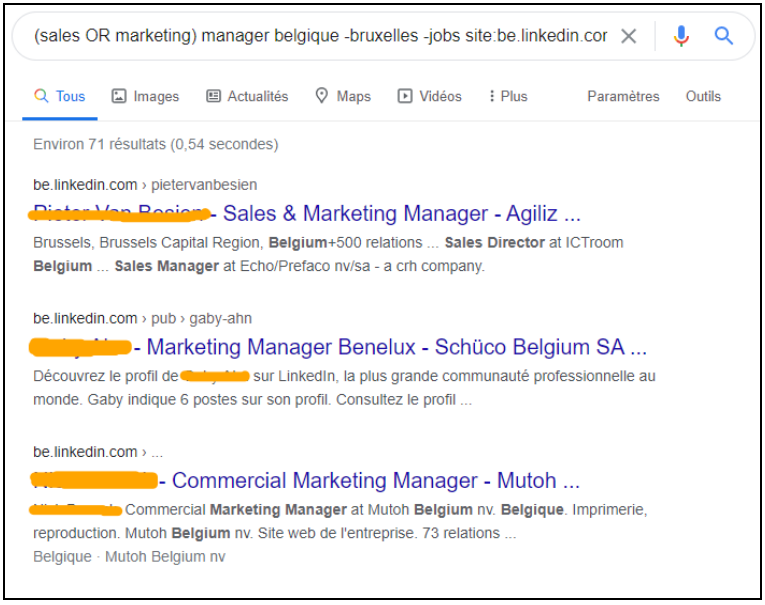
Exemple : Pour élargir considérablement les résultats de votre recherche sur un manager, la recherche de *manag** vous donnera des résultats du type : manager, managing, management, manager etc.

Faites bien attention à l'endroit où vous coupez le mot racine, car l'ajout d'une lettre supplémentaire modifiera vos

résultats. Par exemple, la recherche de manage* éliminera « managing » de la liste originale.

Exclure de votre recherche

Le signe « - « est utilisé lorsque vous souhaitez exclure des termes ou des exigences spécifiques. Dans l'exemple ci-dessous, je recherche un sales manager ou un marketing manager habitant en Belgique mais pas à Bruxelles. Comme je souhaite trouver des candidats potentiels, j'exclus les offres d'emplois. Ici, ma recherche se porte sur le site de LinkedIn.



L'exclusion est surtout intéressante quand vous menez une recherche sur une entreprise mais que vous voulez éviter toutes les pages qui mènent vers le site de cette entreprise.

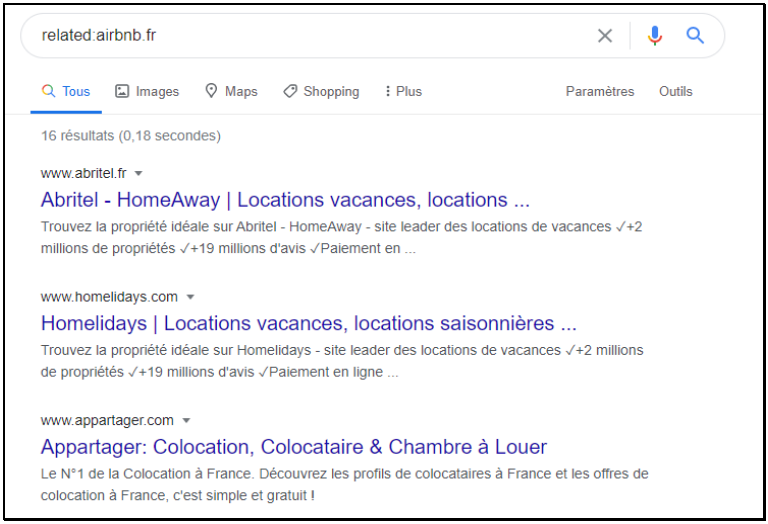
Ici, je veux mener des recherches sur EDF, en évitant les différents sites appartenant à EDF.

Limite des 32 mots

Google ne prend en compte que les 32 premiers mots de vos recherches. Je le dis pour le dire vu que c'est quand même rare de faire une recherche avec plus de 32 mots. Si ça vous semble néanmoins une nécessité, développez votre esprit de synthèse avant de revenir à ce bouquin.

Recherche dans l'environnement d'un concurrent

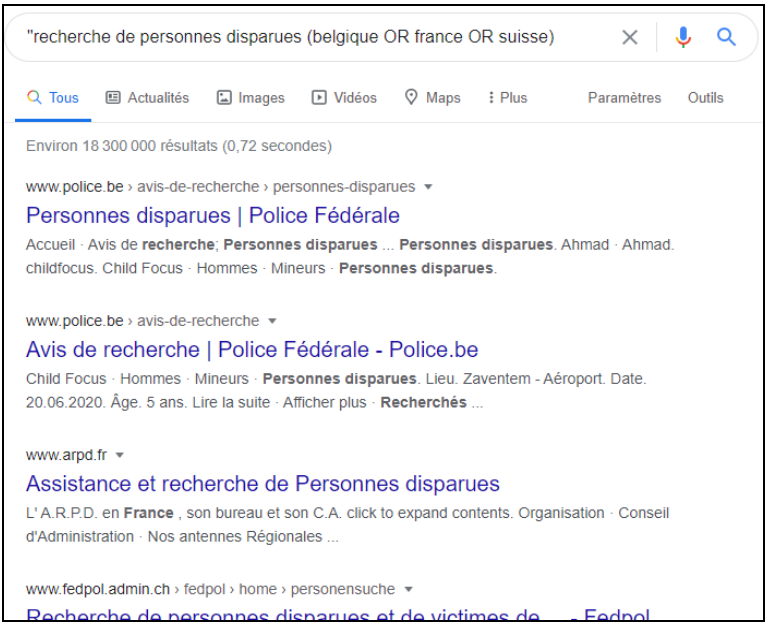
Related est un opérateur qui vous aide à trouver des sites liés à une URL spécifique. L'utilisation de cet outil permet de mieux comprendre comment Google classe votre site web et celui de vos concurrents. Par exemple, si nous examinons les résultats pour airbnb.com, il renvoie les suspects habituels du référencement, mais aussi certains concurrents périphériques pour attirer l'attention.



Cette recherche vous donnera des informations sur l'environnement concurrentiel de votre cible, mais aussi comment Google catégorise votre site. Ici, nous pouvons constater que pour Google, Airbnb est dans l'univers des réservations de vacances en ligne ET dans celui du partage de biens immobiliers.

Mener plusieurs recherches de niveau équivalent

Les parenthèses regroupent des termes ou des opérateurs de recherche pour aider à structurer une recherche avancée.



Google, sans surprise, me propose des liens spécifiques dans les trois pays. Cet opérateur fait gagner beaucoup de temps car quand vous devez mener diverses requêtes de niveau équivalent, vous le faites en une seule fois.

Recherche d'un tarif

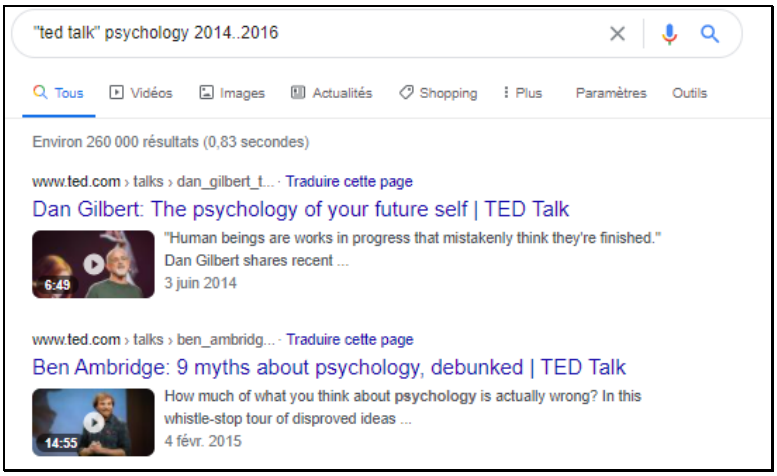
$ / € Cet opérateur vous permet de rechercher le prix d'un produit ou d'un service.

Ici, j'obtiens des tarifs venant de sources neutres ou d'agences de détectives privés.

Lancer une recherche allant de ….à ….

PS4 € 10..80 Ici, je demande les tarifs de la Playstation 4, sachant que je suis disposé à la payer de 10 à 80 euros. Je reçois toute une série de liens vers des consoles d'occasion. Pour ça, je place .. entre deux données chiffrées.

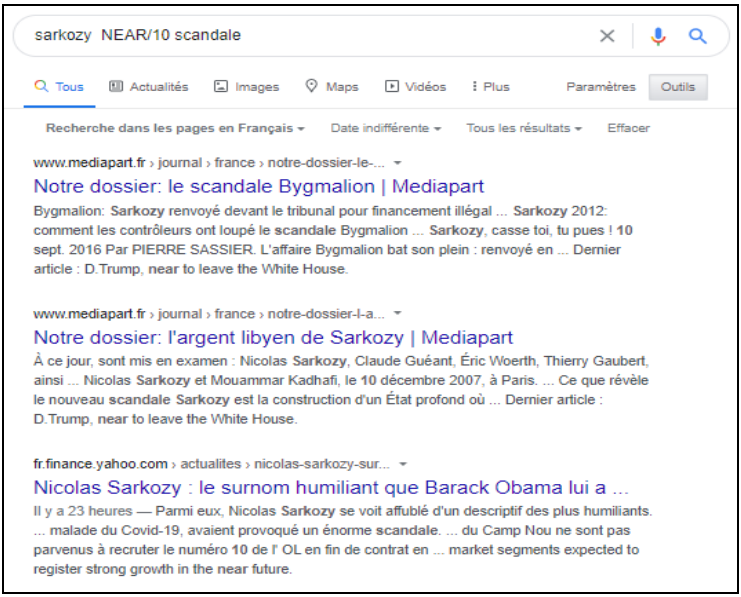
Je pourrais faire la même chose si je cherche les conférences du Ted Talk sur un sujet comme la psychologie de 2014 à 2016. J'obtiens en priorité ce que j'ai demandé. Quand je descends dans la liste, je commence à avoir des conférences Ted qui datent d'autres périodes.



La même technique est envisageable pour la recherche de numéros de cartes de crédit ou des habitants d'une rue donnée.

Recherche de contexte commun

Lorsque vous voulez que deux mots-clés apparaissent à proximité l'un de l'autre dans une série de résultats, vous employez l'expression NEAR/12, ce qui me permet d'obtenir tous les liens où ces mots sont présents, et au maximum, séparés de 12 mots. Bien entendu, vous pouvez utiliser n'importe quel nombre.



Ici, je recherche des informations à propos de scandales liés à Nicolas Sarkozy. Cette option est très intéressante lorsque vous enquêtez sur des liens entre deux entités (personnes, sujets, entreprises…). Ne fut-ce que pour savoir si ces liens existent.

Chercher des fichiers spécifiques

Si votre recherche se limite à un type de fichier en particulier, l'opérateur « filetype » est pour vous. En ajoutant cet opérateur à votre recherche, vous pourrez demander à Google de ne remonter qu'un seul type de fichier dans les résultats. Par exemple, si vous souhaitez des adresses Email de journalistes, mais uniquement sur tableur Excel, cela donnera ceci : *journaliste AND mail filetype:xls*

Cet opérateur ne fonctionne pas avec toutes les extensions de fichiers mais les plus utilisées sont compatibles :

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

GPS eXchange Format (.gpx) soit filetype:gpx

HTML (.htm, .html, et autres extensions) soit filetype:htm

Microsoft Excel (.xls, .xlsx) soit filetype:xls

Microsoft PowerPoint (.ppt, .pptx) soit filetype:ppt

Microsoft Word (.doc, .docx) soit filetype:doc

OpenOffice presentation (.odp) soit filetype:odp

OpenOffice spreadsheet (.ods) soit filetype:ods

OpenOffice text (.odt) soit filetype:odt

Rich Text Format (.rtf) soit filetype:rtf

Text (.txt, .text, et autres extensions) soit filetype:txt

XML (.xml) soit filetype:xml

Recherche dans le titre

L'opérateur intitle: permet de regrouper tous les résultats mentionnant le mot-clé précisé dans le titre de la page

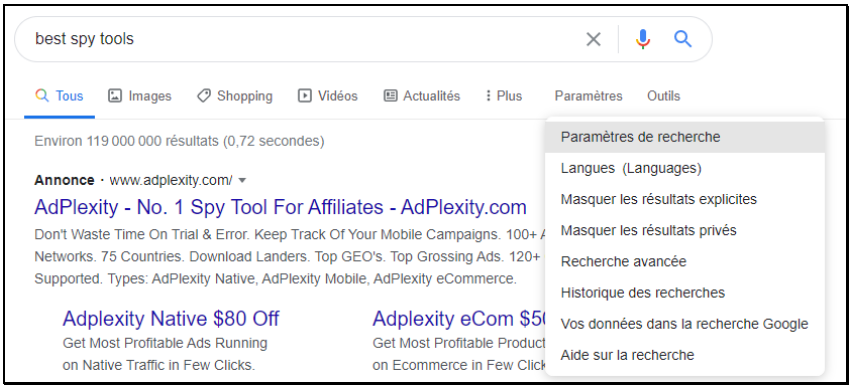
Exemple : *intitle:(espionnage OR renseignement)* me proposera tous les liens vers des pages dont le titre contient le mot « espionnage » ou « renseignement ».

Si vous êtes trop pointu dans une recherche, le risque est que vous n'obteniez rien. Pas grave, il est toujours temps d'élargir les critères. Si vous cherchez des documents sur Volkswagen en allemand sur le territoire du Congo, ça risque de ne pas donner grand-chose de terrible (j'ai essayé, et il y en a quand même un).

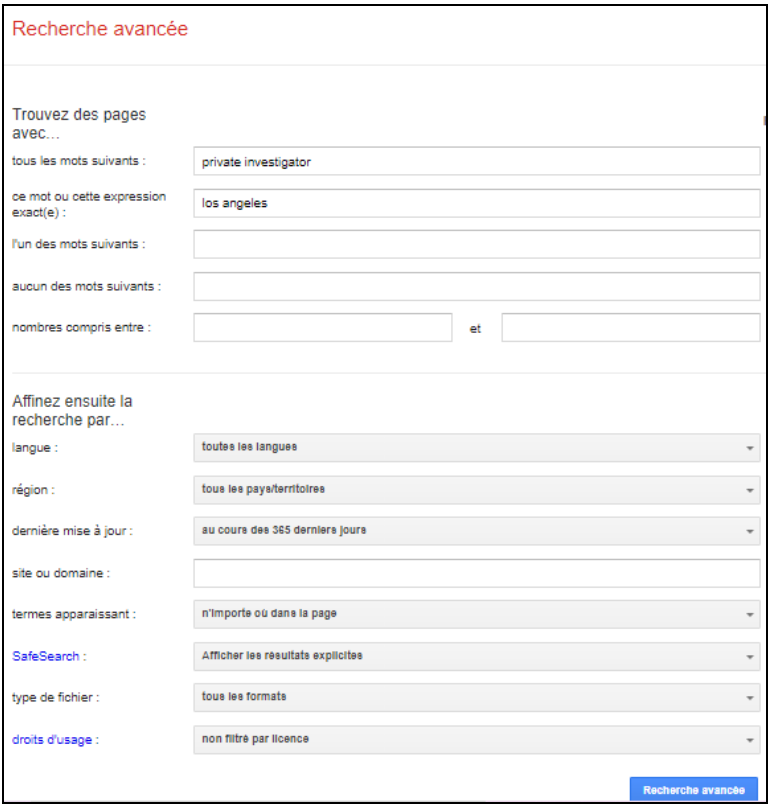
Quand vous souhaitez mener une recherche dans un pays donné, je vous suggère d'utiliser le Google national (google.fr pour la France, google.it pour l'Italie…). Les résultats seront à la fois plus nombreux et mieux structurés. Bref, tous les Google du Monde ne se ressemblent pas.

3. La recherche avancée

La recherche avancée est un peu la version automatisée de la recherche booléenne. Ça fait presque tout. Mais pas tout. Je vous invite à cliquer sur le bouton « recherche avancée ». Que vous trouverez en cliquant sur le bouton « paramètres », puis, « recherche avancée ».



Son principal avantage est de vous éviter l'apprentissage des règles cabalistiques de la recherche booléenne traditionnelle. Mais si vous voulez devenir un vrai champion de la traque à l'info, la recherche avancée ne vous dispense pas d'un travail d'apprentissage.



Dans cette recherche, j'ai besoin de trouver un détective privé dans la région de Los Angeles, Californie. C'est une recherche très simple, et les résultats proposés par Google sont exactement ce dont j'ai besoin. La recherche avancée me propose toutes les combinaisons de « AND » « OR » () – dont je peux avoir besoin. Très pratique. J'aurais aussi bien pu demander de trouver un détective privé en Californie, mais pas à Los Angeles ni à San Francisco.

Le moteur me permet de mener une recherche par langue. Ce qui signifie que si vous ne parlez que le français, rien ne

vous empêche de demander les résultats uniquement en français. Evidemment, avec une recherche de détectives californiens, ça ne risque pas de donner grand-chose. En vérité, rien du tout. De même que si je demande « détective prive » et pas « private investigator ».

Je peux aussi lancer une recherche par région, ce que je vous déconseille de faire car un site peut être hébergé dans n'importe quel pays. Rien ne m'empêche d'avoir un site francophone en Thaïlande (ce qui est justement le cas).

Je peux faire une recherche en fonction de la dernière mise à jour des liens. Cette option est un peu faible car soit vous pouvez demander les résultats de la dernière année, du dernier mois, de la dernière semaine, des dernières 24 heures ou alors vous acceptez que la date vous soit indifférente. Ce qui veut dire que si vous voulez obtenir les résultats des deux dernières années, une fois vos résultats apparus, vous allez devoir cliquer sur le bouton « outil » de Google et demander les résultats en fonction des dates qui vous conviennent.

Si vous n'indiquez rien, « date indifférente » sera le choix par défaut et vous vous ramasserez à peu près tout depuis l'antiquité de Google.

Vous pouvez aussi demander que les termes recherchés apparaissent n'importe où dans la page, dans le titre, dans le texte ou dans l'URL de la page.

Et enfin, vous pouvez demander à ne recevoir que les liens existants dans un format spécifique (Word, Excel, PDF…), ce qui est utile si vous recherchez des rapports ou des bases de données par exemple.

4. Quelques applications offensives avec le Google Hacking

Le Google hacking, appelé aussi Google Dork ou Google dorking est une ressource précieuse pour les enquêteurs. Pour le commun des mortels, Google n'est qu'un moteur de recherche utilisé pour trouver du texte, des images, des vidéos et des informations. Cependant, dans le monde de l'infosecurity, Google est un puissant outil d'investigation.

Vous ne pouvez pas pirater des sites directement en utilisant Google, mais comme il possède d'énormes capacités de

recherche sur le web, il peut indexer presque tout ce qui se trouve sur votre site, y compris des informations sensibles. Cela signifie que vous pourriez exposer trop d'informations sur vos technologies web, noms d'utilisateur, mots de passe et vulnérabilités générales, sans même le savoir.

En d'autres termes, le "Dorking" de Google est la pratique qui consiste à utiliser Google pour trouver des applications et des serveurs web vulnérables. Je ne défonce pas une porte, je me permets de rentrer parce que c'est ouvert.

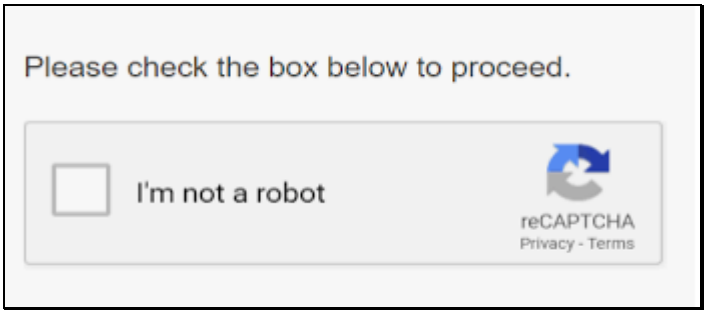
À moins que vous ne bloquiez des ressources spécifiques de votre site web à l'aide d'un fichier robots.txt, Google indexe toutes les informations présentes sur tout site web. Logiquement, après un certain temps, toute personne dans le monde peut accéder à ces informations si elle sait ce qu'elle doit rechercher. Sachez que Google sait également qui vous êtes lorsque vous effectuez ce type de recherche. Pour cette raison et bien d'autres, il est conseillé de ne l'utiliser qu'avec de bonnes intentions, ou si ça n'est pas le cas, avec de bonnes protections.

Bien que certains webmasters exposent par mégarde des informations sensibles, cela ne signifie pas qu'il est légal de tirer profit de ces informations ou de les exploiter. Si vous le faites, vous rentrez dans la catégorie très tendance des cybercriminels.

Un exemple concret : il y a peu, je menais une recherche d'adresses email d'entreprises et de dirigeants d'entreprises. Je suis tombé sur l'index d'un site de vente d'adresses et en creusant l'index, je suis tombé sur une base de données avec 200.000 adresses. Sans doute parce que quelqu'un avait oublié de l'associer à un code d'accès. Je n'ai donc

commis aucune intrusion, mais si j'utilise ces données, ce sera quand même considéré comme du vol. J'ai fait deux choses : une copie de la base pour moi et j'ai prévenu la société qu'il y avait une petite brèche dans leur sécurité.

Avant de poursuivre votre lecture, sachez que Google commencera à bloquer votre connexion si vous vous connectez à partir d'une seule IP statique. Il vous demandera de lancer des défis "captcha" pour empêcher les requêtes automatiques.



Cela se produit très vite lorsque vous faites des requêtes que Google trouve étranges. Quand vous voyez le captcha ci-dessus, pas de panique. Vous cliquez, éventuellement vous répondez à une bête question, et tout repart. Mais c'est un premier signal d'alarme.

Les Google Dorks suivants peuvent être utilisés pour détecter **les serveurs vulnérables ou piratés**

inurl:/proc/self/cwd

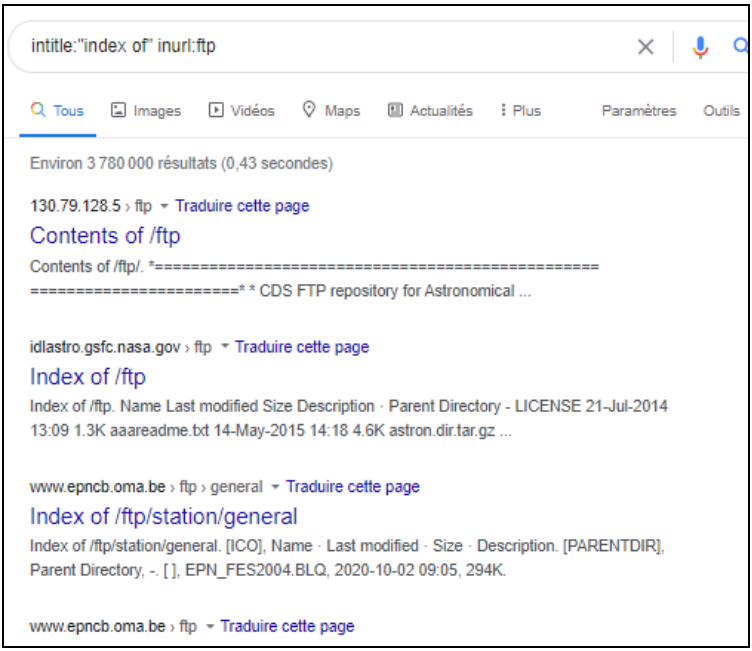
Comme vous pouvez le voir dans la capture d'écran suivante, les résultats des serveurs vulnérables apparaîtront, ainsi que leurs répertoires exposés qui peuvent être

consultés à partir de votre propre navigateur. Il fait bon chez vous.

Google n'indexe pas seulement les serveurs HTTP, il indexe également les serveurs FTP ouverts. Avec le dork suivant, vous pourrez explorer les serveurs FTP publics, qui peuvent souvent révéler des choses intéressantes.

intitle:"index of" inurl:ftp

Vous tombez sur le même genre d'index qu'au point précédent, mais dans la sphère publique.



Vous voyez que le deuxième site dans la capture d'écran ci-dessous est de la Nasa. J'avoue ne pas être entré pour dire bonjour.

Listes d'emails

Il est assez facile de trouver des listes d'emails en utilisant Google Dork. Souvent, ça n'est ni intéressant, ni nuisible. Mais quand vous cherchez des bases de données précises et que vous trouvez tous les emails d'étudiants de telle ou telle école ou du personnel de tel hôpital, ça devient plus délicat. Et j'en trouve des centaines. Sans être un geek, juste en appliquant ce qui se trouve dans ce chapitre. Dans l'exemple

suivant, nous allons chercher des fichiers Excel qui peuvent contenir des emails.

filetype:xls inurl:"email.xls"

Il existe des tas de combinaisons possible pour trouver des mails. Ceci n'est qu'un exemple parmi beaucoup d'autres.

Nous avons filtré pour ne vérifier que les noms de domaine .edu et avons trouvé les adresses de nombreux étudiants, avec leur nom bien entendu.

site:.edu filetype:xls inurl :"email.xls"

N'oubliez pas que la véritable puissance de Google Dork provient des combinaisons illimitées que vous pouvez utiliser. Ma crainte avec ce chapitre est que le lecteur applique sans s'intéresser à la logique. Si vous maitrisez la logique, ce que vous pouvez trouver en termes d'informations est limité uniquement par votre imagination.

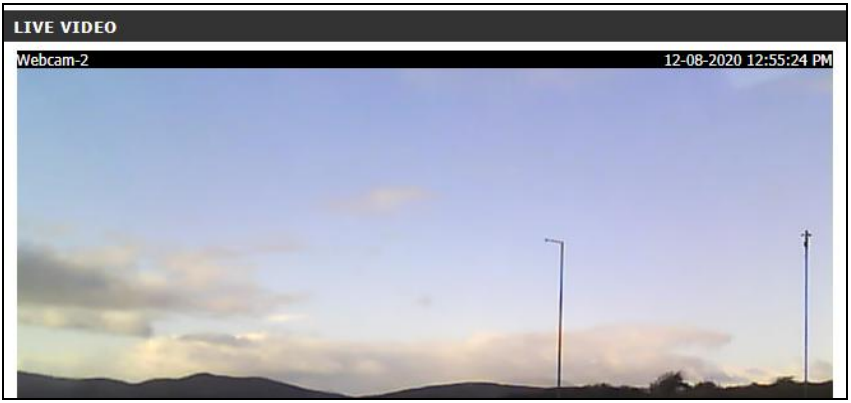
Caméras en direct

Vous êtes-vous déjà demandé si votre caméra privée pouvait être regardée non seulement par vous, mais aussi par n'importe qui sur Internet ?

Les techniques de piratage Google suivantes peuvent vous aider à récupérer les pages web des caméras en direct qui, volontairement ou non, sont accessibles sans mot de passe.

Voici quelques astuces pour accéder à différentes caméras:

inurl:top.htm inurl:currenttime



Il existe, tout comme pour les adresses email, des centaines de combinaisons possibles pour accéder à des caméras vidéo.

Pour trouver les transmissions basées sur la WebcamXP :

intitle:"webcamXP 5"

Ceci est une caméra publique d'une ville polonaise. Comme vous pouvez le voir sur la partie supérieure droite de la photo, je n'ai pas qu'un accès passif à la caméra. J'ai d'ailleurs directement accès à plusieurs caméras de la ville, dont certaines avec des vues en hauteur.

L’option « multi views » me donne un accès simultané à diverses caméras publiques de la ville. Rien à dire, on se sent en sécurité. Et un autre pour les caméras générales en direct :

inurl : "lvappl.htm"

Il y a beaucoup de caméras live qui peuvent vous permettre de regarder n'importe quelle partie du monde, en direct. Vous pouvez trouver des caméras éducatives, gouvernementales et même militaires. Dans un autre registre, j’ai trouvé un site qui cartographie les sites militaires du monde entier, avec vues satellites. Leur ambition n’est pas l’espionnage, mais le jeu. Ils s’amusent. Là où ça devient moins drôle, c’est que ces braves petits gars veulent montrer leur boulot et que n’importe qui peut utiliser leur hobby favori à des fins plutôt fatales.

Si vous êtes créatif, vous pouvez même faire des tests de pénétration sur ces caméras. Vous serez surpris de voir comment vous pouvez prendre le contrôle du panneau d'administration complet à distance, et même reconfigurer les caméras comme vous le souhaitez. En utilisant ces clés,

vous tomberez souvent sur des webcams volontairement accessibles à tout le monde, souvent à des fins touristiques. Du coup, pas de problème. Mais quand au bout de deux minutes, je me retrouve derrière des caméras de sécurité au cœur des villes ou des entreprises, je suis à la fois excité par le jeu, et anxieux de la fragilité de nos systèmes d'informations.

A titre informatif, voici une liste de clés pour accéder à des caméras publiques. C'est certes amusant et impressionnant. Mais n'oubliez pas que c'est totalement illégal et que vous serez facile à identifier. Si vous prenez le contrôle de la caméra d'un parking en Alabama, le risque est modéré, tout comme si vous vous retrouvez dans la salle d'attente d'un dentiste népalais. Si vous accédez à un site de missiles nucléaires sibériens, je serais moins sûr.

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"

Vous trouverez ici http://cinemauniversaldownloads.blogspot.com/p/blog-page_16.html une liste impressionnante et pourtant non-exhaustive de clés vous permettant d'accéder à des caméras. Cela semble aléatoire et avec ces codes, ça l'est. Rien ne vous empêche de rajouter des critères de précision, comme une ville par exemple. Dans ce cas, nous reprenons le cours de ce livre : un outil de renseignement actif et offensif.

Enfin, Camhacker et Insecam sont deux moteurs de recherche de caméras IP non protégées. Vous pouvez mener des recherches par lieux, par types de caméra, par thème…et à chaque fois, j'ai une localisation de la caméra avec longitude et latitude. Nous avons là un véritable outil de renseignement, précis et mis à jour. Les codes du hacking Google, c'est génial, mais vous allez surtout où on vous emmène. Il est difficile de mener une recherche sur un endroit précis, alors qu'avec ces deux sites, c'est tout à fait possible. Beaucoup de caméras sur ces deux sites sont des webcams volontairement publiques. Il n'y aura pas grand-chose à en tirer. En revanche, il y a aussi beaucoup de ces caméras qui sont des caméras de ville et qui vous permettent alors une excellente observation d'une zone.

http://insecam.org/

https://www.camhacker.com/

Un peu plus loin, vous trouverez des informations sur l'outil « Shodan » qui peut aussi vous aider à trouver des caméras.

5. Localiser un lieu ou une personne avec une photo

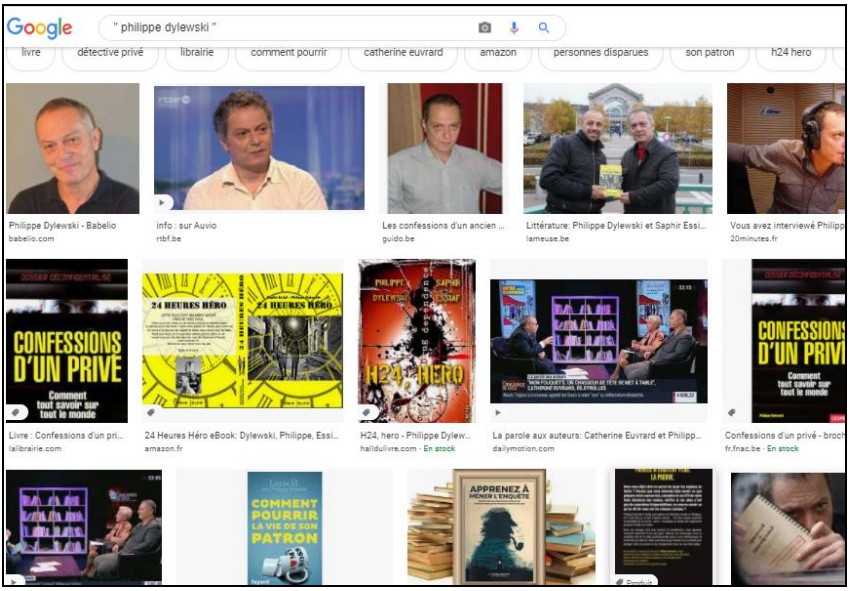
La recherche d'images la plus complète sur le Web. C'est ce que dit GOOGLE en parlant de lui-même. Ça a certainement été vrai. Peut-être que ça l'est encore. Mais si vous devez enquêter sur une image, le monopole de Google est terminé.

Google Images est utile dans la recherche d'informations professionnelles à plusieurs titres, même si rien de révolutionnaire en termes de résultats ne doit être attendu.

En recherche de personne, c'est très chouette. Tapez le nom de votre cible (le dirigeant de votre concurrent ou l'un de ses commerciaux par exemple) et vous avez de bonnes chances de visualiser sa bobine chérie. Si vous avez vraiment du bol, vous verrez que d'autres photos apparaissent. Google cherche large et vous verrez alors des photos relatives à votre cible : personnes ayant votre cible comme amis sur Facebook, collègues, famille, etc.

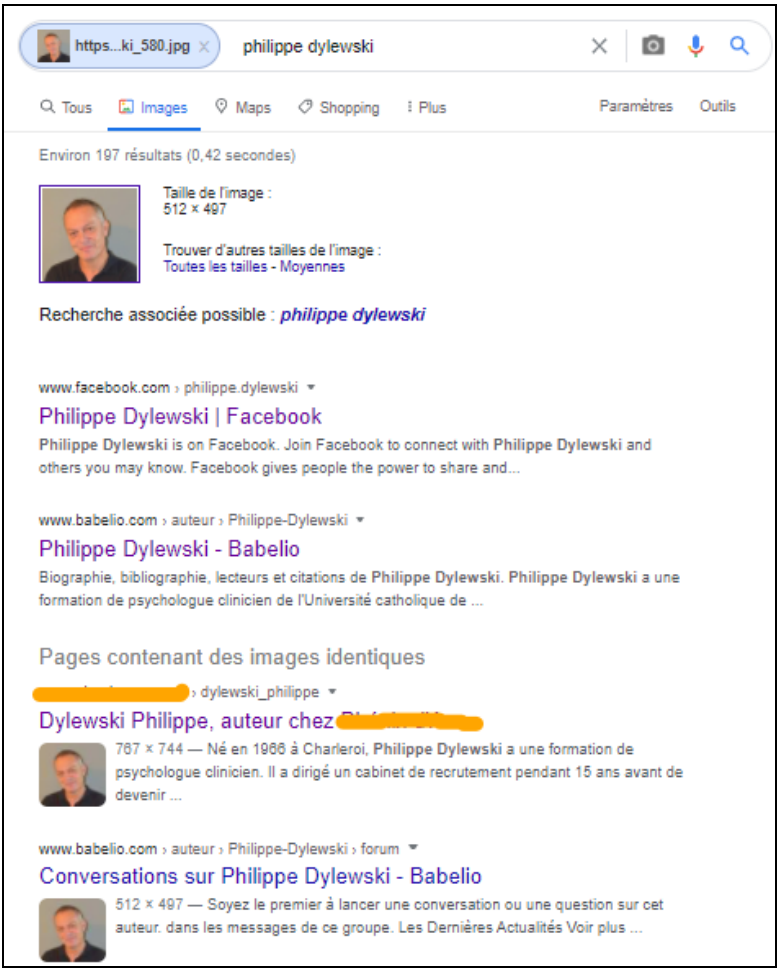
Mais si vous recherchez de l'info sur une société ou un produit, il y a de la richesse ici aussi. Amusez-vous à taper « EDF » ici et vous verrez bien entendu des tonnes de logos EDF, mais aussi des pubs, campagnes d'affichages, couvertures de manuels, documents scannés, photos de sites, organigrammes. Google images a aussi des applications plus poussées dans le monde du renseignement. Vous pouvez retrouver l'origine d'une image, en tout cas si elle est diffusée dans plusieurs endroits.

Dans un moment de délire mégalomaniaque, je mène une recherche sur moi-même.



Parfait, je suis rassuré, on parle de moi. Mais soudainement inquiet, je veux savoir si ces photos n'ont pas été diffusées à mon insu.

Je clique alors sur la photo qui m'intéresse jusqu'à ce que je me retrouve sur le site où elle a été publiée, puis je pointe ma souris sur la photo, clique sur le bouton de droite de ma souris et un nouveau clic sur « search Google for image ».



C'est officiel, je ne suis pas si célèbre que ça. Cependant, Google Images retrouve la trace de cette photo sur 3 sites, dont Facebook.

Vous pouvez aussi faire une recherche à partir de photos stockées dans votre ordinateur. Pour ça vous cliquez sur l'appareil photo en haut à droite de votre page et Google

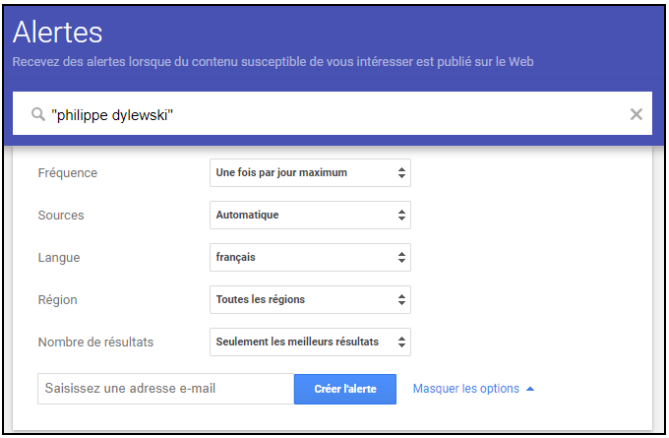
images vous propose de télécharger une photo à partir de vos dossiers.

Pas trop de miracle à attendre ici en recherche de personnes disparues. Parce que si la photo en votre possession n'a pas été publiée sur un site, forcément, vous n'obtiendrez rien du tout.

6. Être prévenu en temps réel de tout changement chez votre cible

Google Alert vous prévient de toute modification de contenu de votre cible, en temps réel si vous le voulez. C'est simple, c'est gratuit, c'est efficace. Vous pouvez lancer autant de requêtes que ça vous chante.

https://www.google.fr/alerts



Vous pouvez l'utiliser pour :

- Savoir ce que l'on dit de vous

- Suivre les nouveautés chez votre concurrent
- Vous tenir informé de ce qui se dit sur vos concurrents
- Être informé de toute nouveauté sur un thème

Mes bouquins sont souvent piratés par des sites qui en proposent le téléchargement « gratuit ». Presqu'à chaque fois, ça n'est qu'une arnaque, mais je veux me tenir au courant. Avec Google Alert, je suis prévenu en temps réel dès qu'un site fait mention d'un livre que j'ai écrit. Cela étant, je décide de réagir, ou pas. Mais au moins, je suis informé.

Pour les détectives privés, l'outil peut aussi avoir son utilité en recherche de personne. Si vous avez fouillé la planète pour retrouver votre cible, sans succès, il vous reste à attendre qu'elle fasse parler d'elle. Taper le nom de votre cible ici, et peut-être qu'un jour, ça va marcher. On est d'accord, la probabilité est faible et pourtant ça reste indispensable de le faire.

Avec Wysigot, vous placez le site de votre concurrent en veille et êtes informé de toute modification de son site. Comme il s'agit d'un navigateur offline, vous devez télécharger une application.

http://www.wysigot.com

7. Google Video

Il existe des tas de moteurs de recherche de vidéos. J'en ai testé quelques-uns et c'est GOOGLE VIDEO (http://video.google.fr) qui emporte la palme, largement. Ça m'embête, car le monopole est quelque chose qui me dérange. Pour ma petite satisfaction, je constate quand même que dans certains domaines, Google n'est plus ce qui se fait de mieux.

Google Vidéo va aller chercher ce qui vous intéresse sur une série de sites dédiés aux vidéos : YouTube, Dailymotion, chaînes de télévision et autres. Encore une fois, Google enregistre toutes vos recherches.

A quoi ça sert d'aller chercher des vidéos sur un concurrent ou un partenaire ?

- Voir les pubs réalisées par la compagnie.
- Voir les reportages provenant de chaînes de télévision.
- Voir les films réalisés par les détracteurs de la compagnie (dans ce cas-ci, c'est facile, EDF n'en manque pas).
- Visiter les installations.
- Identifier des personnes clés.

Pour un espion, c'est la gloire, car vous trouverez peut-être des vidéos réalisées par des employés de votre concurrent, avec un peu de chance à l'intérieur même des bâtiments.

Mais ce n'est pas tout, non, non. Google Vidéos propose aussi des options de recherche avancée. Je ne vais pas m'étaler pendant dix pages, mais il y a quand même quelques fonctions utiles, puisque vous pouvez faire un tri en fonction de critères vraiment pertinents comme des combinaisons de mots clés dans une recherche classique sur le web, ce qui permet d'affiner quand vous obtenez trop de résultats.

Ex-Recherche par langue et par pays.

Ex-Durée de la vidéo.

Ex-Par date (quoi que l'option soit fort limitative).

8. Comment trouver très vite un mot en particulier sur une page web ?

Vous faites une recherche dans un article très long et un seul mot vous intéresse, le nom de votre cible par exemple. Ou vous cherchez une série de chiffres dans un code gigantesque.

Tapez « ctrl F » et dans l'exemple ci-dessous, vous voyez que le mot est aussitôt détecté et placé en surbrillance.

Ce petit truc vous aide surtout à gagner un temps précieux.


carte sim
1/18
CARTE SIM EN
ACCUEIL » SIN CATEGORIZAR » CONSEILS DE VOYAGE »
CONSEILS POUR CHOISIR VOTRE CARTE SIM EN THAÏLANDE
COMMENT CHOISIR VOTRE CARTE SIM EN THAÏLANDE
De nos jours, il est très courant et très pratique de prendre une carte sim du pays lorsque vous
Thaïlande. Elle vous permettra d'avoir une numéro de téléphone local et vous pourrez passer

III. La puissance de la recherche OSINT

Lorsqu'on parle d'OSINT (open source intelligence), on peut avoir le sentiment que puisque c'est accessible, ça ne vaut rien. Que pour qu'une information soit valable, il faut l'avoir trouvée de façon illégale. Le principe selon lequel ce qui est coûteux en temps, en énergie ou en argent, a de la valeur.

Les renseignements provenant de sources ouvertes vous permettent dans la majorité des cas, de trouver votre bonheur. Car si l'information est accessible, cela ne veut pas dire qu'elle soit facile à trouver. Il ne suffit pas de le dire, je vais tâcher de vous en convaincre dans ce chapitre.

Les agences militaires américaines ont commencé à utiliser le terme OSINT à la fin des années 1980 alors qu'elles réévaluaient la nature des besoins en informations aux niveaux tactiques sur les champs de bataille. Puis, en 1992, la loi sur la réorganisation des services de renseignement a déterminé que les principaux objectifs de la collecte d'informations comprenaient des concepts clés comme :

- Le renseignement doit être objectif et sans parti pris

- Les données doivent être disponibles sur des sources publiques et non publiques

Bien que le concept d'OSINT ait évolué depuis lors, puisqu'il n'inclut pas les sources non publiques, le concept est issu de cette époque.

Les renseignements de source ouverte (OSINT) sont des informations recueillies auprès de sources publiques telles que celles disponibles sur Internet, bien que le terme ne soit pas strictement limité à Internet, mais désigne plutôt toutes les sources disponibles publiquement.

"OS" (de OSINT) signifie Open Source. Dans ce cas, il n'est pas lié au fameux mouvement open source qui propose des logiciels libres d'accès, mais à toute source publiquement disponible où l'utilisateur peut obtenir les informations dans sa collecte de données de renseignement. Le mot clé derrière le concept OSINT est l'information, et plus important encore, l'information qui peut être obtenue gratuitement ou presque. Peu importe qu'elle se trouve dans des journaux, des blogs, des pages web, des tweets, des réseaux sociaux, des images, des podcasts ou des vidéos, tant qu'elle est publique, gratuite et légale. En réalité, aucun de ces critères n'est absolu.

Avec les bonnes informations entre les mains, vous pouvez obtenir un grand avantage sur vos concurrents ou accélérer les enquêtes sur les entreprises et les personnes dont vous êtes responsable. Les entreprises et les particuliers utilisent l'OSINT toute la journée, sans le savoir consciemment. Les équipes de vente, de marketing et de product management utilisent également l'OSINT pour augmenter les conversions ou simplement être plus efficaces dans la vente de leurs services au public.

Que vous meniez une enquête de cybersécurité contre une entreprise ou une personne, ou que vous soyez à l'opposé en train de travailler à l'identification et à l'atténuation des menaces futures, le fait d'avoir des techniques OSINT

prédéfinies et des objectifs clairs peut vous faire gagner beaucoup de temps.

La plupart des sociétés n'adoptent pas l'OSINT pour renforcer leurs défenses contre les cyberattaques. C'est parfait, cela nous arrange. Que ce phénomène existe par négligence, ignorance ou condescendance m'importe peu. Les failles de nos cibles sont les armes du renseignement. Bien qu'il existe de nombreuses techniques d'OSINT, elles ne fonctionneront pas toutes pour votre cible. Tout d'abord, vous devrez vous poser quelques questions :

- Qu'est-ce que je cherche ?

- Quel est mon principal objectif de recherche ?

- Quelle est ma cible ou qui est ma cible ?

- Comment vais-je mener mes recherches ?

Essayez de trouver la réponse à ces questions, et ce sera la première étape de votre enquête OSINT. Bien que de nombreuses techniques OSINT soient utilisées par les agences gouvernementales et militaires, elles peuvent souvent être appliquées dans le secteur privé. Certaines peuvent fonctionner, d'autres pas, mais cela fait partie de la stratégie de l'OSINT - vous devrez identifier les bonnes sources et celles qui ne sont pas pertinentes pour votre recherche.

1. Risques liés à la réalisation d'une enquête OSINT

Je divise cette préoccupation en trois risques distincts :

- Le risque d'être détecté : Il s'agit du contact direct établi en utilisant des techniques actives, ou des services de tiers qui peuvent vous faire découvrir. Si votre mission consiste à collecter des informations sur un fabricant de piscine à l'autre bout du pays, être découvert ne vous causera probablement pas grand dommage. Si vous cartographiez en profondeur le réseau nucléaire français pour le compte d'une puissance étrangère, le risque est un peu plus élevé et les conséquences, potentiellement dramatiques pour vous.

- Risque de perdre l'accès à ces informations : Une fois qu'ils savent que vous suivez leurs pas ou que vous recherchez leurs informations, ils peuvent commencer à effacer leurs propres traces et fermer l'accès aux données publiques.

- Risque de devenir la victime : Après tout, vous pouvez finir par être la cible d'une enquête, ou pire encore, l'organisation à laquelle vous appartenez peut subir ce sort. Il convient de faire preuve d'une grande prudence lors de l'utilisation des techniques actives d'OSINT. Surtout si vous utilisez aussi les autres stratégies proposées dans ce livre.

L'OSINT, ce sont avant tout des outils et des techniques. Nous allons en voir quelques-uns. Il en existe des milliers.

Le premier et le plus puissant de ces outils ne sera que cité ici. Ce qu'on peut faire avec Google a déjà été vu dans un chapitre précédent. C'est le cas d'autres outils vus dans

d’autres chapitres, notamment la recherche d’informations sur vos concurrents. J’ai une grande confiance dans l’intelligence du lecteur et sa capacité à aller chercher ce dont il a besoin.

Dernière chose dont on ne parlera pas dans ce chapitre, ce sont les outils morts. Ils sont nombreux et la bataille de l’OSINT en tue chaque jour. Concrètement, si je parle d’un outil dans ce chapitre, c’est qu’il fonctionne et que je l’ai utilisé. Il se peut qu’entre le moment où j’ai utilisé l’outil pour la dernière fois et celui où vous lisez ce chapitre, certains liens soient morts. Pour pallier ce problème, j’ai trouvé deux moyens. Le premier, c’est que si vous tombez sur un lien mort, auriez-vous l’immense bonté de me le signaler ? Le deuxième, c’est que ce livre ne sera tiré que par 100 ou 200 exemplaires à la fois, de façon à être remis à jour en permanence.

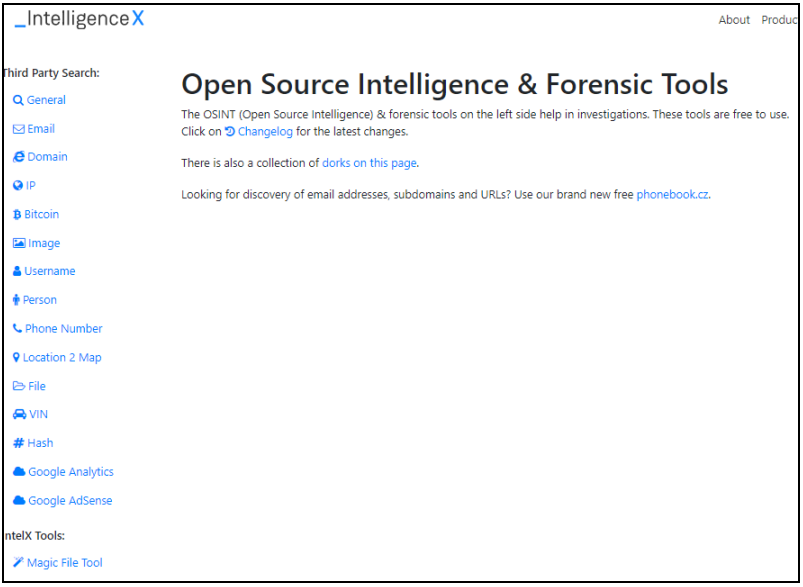
Bon, on y va…

2. Outils d’OSINT

Bien qu'Intelligence X ne soit pas un outil à exécuter sur vos serveurs, puisqu’il s’agit d’un site, c'est un moyen très utile d'obtenir des informations précieuses en interrogeant des moteurs de recherche gratuits, des ressources et des outils disponibles sur Internet. Ils visent à fournir les meilleurs liens vers des sources de données OSINT utiles. La plupart des sites web qu'elle utilise sont gratuits, mais certains peuvent nécessiter le paiement d'une faible redevance.

L'Intelligence X est un arbre aux milles branches. Il est la mère et le père du renseignement. Il est la structuration du grand « tout » de l'information stratégique. Il aborde des dizaines de thèmes, qui eux-mêmes se subdivisent en sous-groupes, qui vous amènent vers une application. Nous allons en voir quelques unes. Les plus intéressantes, celles qui ne sont pas déjà tombées au champ d'honneur du web et aussi celles qui fonctionnent en Europe, car bon nombre d'outils sont excellents mais ne fonctionnent qu'en Amérique du Nord. Si vous voulez tout tester, vous en aurez pour des jours. Mais c'est passionnant.

https://intelx.io/tools



Pour rappel, quand je ne parle pas d'un outil du répertoire Intelligence X, c'est soit parce qu'il est mort, soit parce

qu'il ne donne rien de terrible, soit parce que vous devez passer au travers d'épreuves d'inscription nébuleuses avant d'apprendre que finalement, non, ça n'est pas gratuit car pour être membre Prémium, il faut payer la modeste somme de…

Il y a aussi le cas où l'outil m'est à la fois inconnu et incompréhensible. Ce qui sera votre cas aussi si vous n'êtes pas un champion en sécurité informatique.

Ici, vous pouvez lancer une recherche à travers toute une série de moteurs. La tentation sera grande de les sélectionner tous dans l'espoir d'avoir un maximum de résultats, mais ça n'est pas efficace car si vous sélectionnez cette option, la recherche se fera uniquement à partir du premier moteur coché. Vous êtes un bon petit soldat du renseignement et vous mènerez votre recherche moteur après moteur.

On ne perd pas son temps. Aucun des outils ne fonctionne correctement.

Déjà on commence fort avec l'application *Phonebook* qui me trouve plus de 150 emails appartenant à des collaborateurs du journal belge « Le Soir ». Comme je suis

un vilain spammeur, je peux affirmer que c'est puissant. Je l'ai utilisé pour rechercher des Emails appartenant à d'autres sociétés, et c'est de loin le meilleur.

Avec *Whoxy*, je connaitrai la date de création du site (bof) mais aussi les autres noms de domaines déposés. Du coup, si ma cible a déposé société.be et .fr et a oublié de déposer .com, je peux acheter ces différents noms de domaine et en faire l'usage qu'il me plait.

Avec *Who.is*, je reçois beaucoup d'informations sur les aspects techniques du site.

Portscan est un outil pour les vilains garnements car il recherche les ports ouverts sur un serveur.

OpenLinkProfiler est un outil de recherche de liens qui vous permet de vérifier gratuitement les backlinks de n'importe quel site web. Il vous suffit d'entrer le nom de domaine dans le champ de recherche de l'outil et celui-ci commencera à analyser le site web et vous fournira un rapport complet de ses liens de retour. Gratuit pour le moment. Ça ne durera pas.

Voilà pour quelques outils d'Intelligence X. Il y en a tellement, allez voir, fouillez, c'est immense.

BuiltWith est un moyen efficace de détecter quelles technologies sont utilisées sur n'importe quel site web sur Internet. Il comprend des informations détaillées sur les CMS utilisés comme Wordpress, Joomla, Drupal, etc…, ainsi que des bibliothèques Javascript et CSS complètes comme jquery, bootstrap/foundation, des polices externes, le type de serveur web (Nginx, Apache, IIS, etc.), le fournisseur SSL et le fournisseur d'hébergement web utilisé.

BuiltWith vous permet également de trouver quelles sont les technologies les plus populaires actuellement ou celles qui sont en train de devenir tendance. Il s'agit sans aucun doute d'un très bon outil de veille open source permettant de rassembler tous les détails techniques possibles sur n'importe quel site web.

https://builtwith.com/

SpiderFoot est un outil d'automatisation et de reconnaissance OSINT, dont le but est d'automatiser le processus de collecte de renseignements sur une cible donnée (adresse IP, nom de domaine, nom d'hôte, sous-réseau, ASN, etc.).

Vous pouvez l'utiliser afin de recueillir des informations sur n'importe quelle cible, comme par exemple : DNS, Whois, pages web, DNS passif, listes noires de spam, métadonnées de fichiers, listes de renseignements sur les menaces ainsi que des services comme SHODAN, HaveIBeenPwned (votre adresse mail est-elle compromise ?), etc… mais vous pouvez également essayer cet outil contre votre propre réseau pour voir quelles informations vous donnez.

- abuse.ch - Vérifiez si un hôte/domaine, une IP ou un bloc de réseau est malveillant selon abuse.ch.
- Base64 - Identifier les chaînes codées en Base64 dans tout contenu et URL, révélant souvent des informations cachées intéressantes.

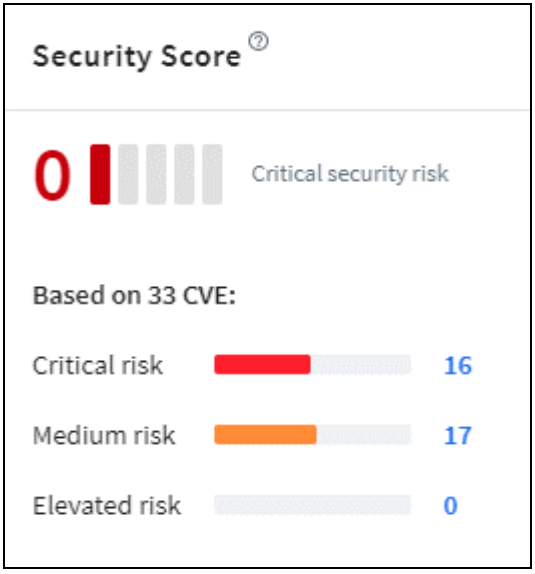
- Blockchain - Interrogez blockchain.info pour trouver le solde des adresses de portefeuilles de bitcoins identifiés.
- cybercrime-tracker.net - Vérifier si un hôte/domaine ou une adresse IP est malveillant selon cybercrime-tracker.net.
- DNS Raw Records - Récupère des enregistrements DNS bruts.
- Google Maps - Identifie les adresses physiques potentielles et les coordonnées de latitude/longitude.
- HackerTarget.com - Recherche sur HackerTarget.com d'hôtes partageant la même adresse IP.
- malwaredomainlist.com - Vérifiez si un hôte/domaine, une IP ou un bloc réseau est malveillant selon malwaredomainlist.com.

Et bien d'autres choses encore. SpiderFoot a cependant un gros inconvénient pour la majorité des lecteurs de ce livre : les résultats sont incompréhensibles pour le commun des mortels. Beaucoup d'outils d'automation en OSINT demandent des compétences techniques. Si vous travaillez dans une grosse structure, vous aurez l'aide de votre IT manager. Si vous êtes actif dans une petite compagnie, vous devrez faire appel à l'extérieur. Lors de la première édition de ce livre, il y a dix ans, la technologie internet était déjà bien présente dans le monde du renseignement, mais à un niveau que j'ai pu rapidement maitriser. Ce n'est plus le cas aujourd'hui. Bien sûr, je pourrais apprendre, et il me

faudrait sans doute quelques mois pour arriver à un certain niveau. J'ai fait le choix de faire appel à des gens plus compétents que moi pour les sujets que je ne domine pas.

https://www.spiderfoot.net/

Pour l'agent de renseignement qui est à la recherche des failles d'un site, Spyse est parfait. Il détecte les vulnérabilités en quelques secondes et vous pouvez l'essayer gratuitement.

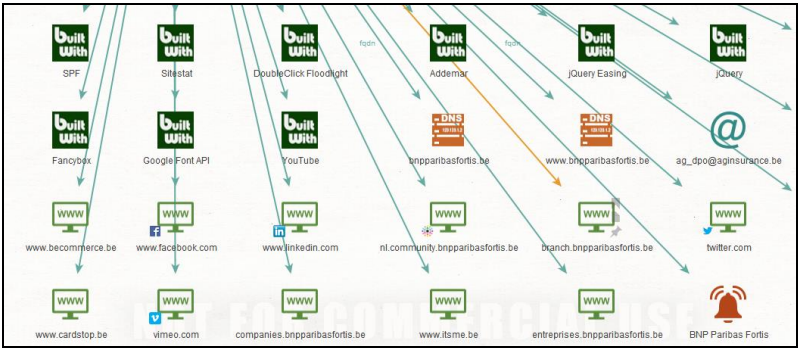


https://spyse.com/

Maltego est un outil d'exploration de données qui exploite une variété de ressources de données open-source et utilise

ces données pour créer des graphiques permettant d'analyser les connexions. Les graphiques vous permettent d'établir facilement des liens entre des informations telles que le nom, la structure organisationnelle, les domaines, les documents, etc... En gros, il analyse une grande quantité d'informations, puis lance un joli graphique qui vous aidera à rassembler les pièces du puzzle. Maltego peut être utilisé comme ressource à tout moment de l'enquête, mais si votre cible est un domaine, il est judicieux de commencer à cartographier le réseau avec Maltego dès le début.

Vous avez une version gratuite qui est déjà impressionnante. C'est surtout le visuel qui tape. Ça donne vraiment le sentiment d'être au cœur de quelque chose, quand on voit les connections existantes entre tous les éléments du tableau.



L'autre aspect important, c'est qu'il s'agit d'une magnifique structuration de l'information. Et chaque fil de la toile peut à son tour être approfondi. Le soft est à télécharger après inscription. Il est assez facile à prendre en main, mais si vous tentez l'aventure sans tutorial, vous ne comprendrez rien. Enfin moi, je n'ai rien compris. Alors

qu'après avoir regardé deux ou trois vidéos de quelques minutes, j'étais parti. Certains disent que c'est l'un des meilleurs outils d'OSINT au monde. C'est un outil pour les professionnels de la veille ou de l'intelligence économique. Si vous êtes le gérant d'une superette et que vous suffoquez parce que votre concurrent vend ses artichauds 12 cents moins chers que les vôtres, utiliser Maltego, c'est un peu comme tirer sur une fourmilière au bazooka. Mais si vous êtes un consultant avec des clients très chics, vos clients sauront avec certitude que vous êtes le nouveau 007 du B2B.

Https ://www.maltego.com/

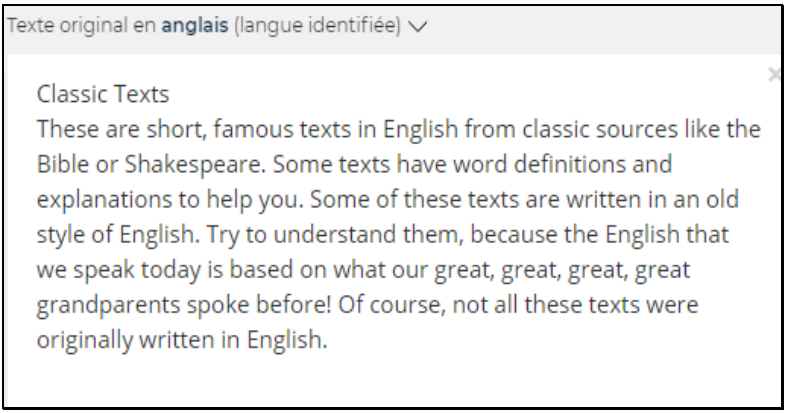
3. Traduire vos documents parfaitement grâce à l'intelligence artificielle

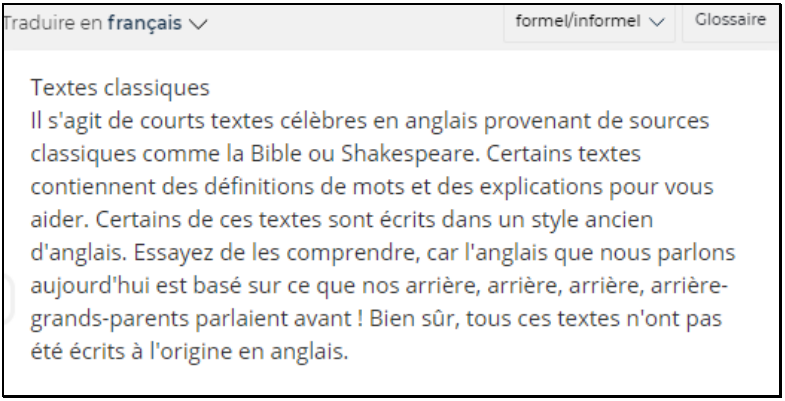
Jusqu'à présent, la traduction était un problème quasi infranchissable. L'outil de traduction de Google, Google translate, est bien gentil, mais d'une efficacité plus que limitée. Maintenant, il existe un outil de traduction en ligne absolument fabuleux.

DeepL est ce qu'on peut appeler un traducteur intelligent. Il tient compte du contexte. Il ne traduit pas littéralement comme les autres traducteurs automatiques, mais trouve le sens du texte. Est-ce une traduction parfaite ? Nos traducteurs diplômés sont-ils priés de se reconvertir dans l'heure ? Non, mais on s'en approche doucement.

Pour vos enquêtes dans des langues qui vous sont étrangères, c'est tout à fait parfait. La barrière de la langue

n’existe tout simplement plus. Et si vous devez rédiger un document, DeepL est d’une grande aide car ce que vous écrirez sera tout à fait compréhensible pour votre interlocuteur. L’outil ne fonctionne qu’avec un nombre limité de langues : le français, l’anglais, le néerlandais, l’allemand, l’italien, l’espagnol, le portugais, le chinois, le japonais, le russe et le polonais.





Je vous invite à comparer les deux textes. Le texte source est en anglais.

Pour ne rien gâcher de la joie d'avoir trouvé un traducteur de ce niveau, il est gratuit pour des textes ne dépassant pas 5000 signes, ce qui fait quand même plus ou moins trois pages.

https://www.deepl.com/

4. Le moteur de recherche pour les hackers et l'art d'entrer par les portes laissées ouvertes (oups)

Shodan est un moniteur de sécurité réseau et un moteur de recherche axé sur le deep web et l'internet des choses. Il a été créé en 2009 pour suivre les ordinateurs accessibles au public à l'intérieur de n'importe quel réseau.

Il est souvent appelé le "moteur de recherche des hackers", car il vous permet de trouver et d'explorer différents types de dispositifs connectés à un réseau comme les serveurs, les routeurs, les webcams, les imprimantes etc.…Mais ce sera bientôt le cas aussi de votre grille-pain, de votre télé ou de votre climatisation.

Shodan est à peu près comme Google, mais au lieu de vous montrer des images, des textes, des vidéos et des sites web riches en contenu, il vous montrera des choses qui sont plus en rapport avec l'intérêt des chercheurs en sécurité informatique, comme les bannières de serveurs SSH, FTP, SNMP, Telnet, RTSP, IMAP et HTTP et les informations

publiques. Les résultats seront présentés par ordre de pays, de système d'exploitation, de réseau et de ports.

Les utilisateurs de Shodan ne sont pas seulement en mesure d'accéder à des serveurs, des webcams et des routeurs. Il peut être utilisé pour scanner presque tout ce qui est connecté à l'internet. Regardez chez vous ou autour de vous ce qui est connecté et tremblez.

On peut se dire que Shodan est l'outil parfait du geek et uniquement pour le geek. Qui passe ses nuits à chercher les failles de sécurité d'un réseau. C'est vrai. Mais c'est aussi un outil puissant pour un enquêteur qui a dorénavant accès à toute la connectivité d'une cible. Mais le Graal est pour le responsable marketing. Ce qui est un peu plus inattendu.

Les appareils connectés affichent leurs marques et numéros de modèle directement sur les pages de connexion et dans les en-têtes http. A partir de là, on pourrait imaginer que Shodan détecte les marques et modèles de vos appareils connectés, de plus en plus nombreux. Je vous laisse imaginer la suite.

En tant qu'outil, Shodan est plutôt facile à prendre en mains. Après tout, ça n'est qu'un moteur de recherche. A partir de la fonction « explore », en haut de l'écran, vous pourrez assez vite comprendre le fonctionnement de l'outil. Mais si vous n'êtes pas un afficionado du net, c'est l'interprétation des résultats qui sera problématique.

La question de la légalité de Shodan se pose. Oui, Shodan est légal. Après tout, il ne fait que trouver des failles et les compiler. Ce que d'autres méthodes permettraient de faire.

Là où Shodan risque de tomber dans l'illégalité, c'est surtout ce que vous en ferez.

Le prix : si vous faites une recherche ponctuelle, l'accès à Shodan est gratuit. Dès que vous voulez en faire un outil de recherche plus pointu et régulier, il faudra payer. A partir de 59 dollars par mois.

https://www.shodan.io/

Angry IP scanner est un scanner de réseau rapide et convivial pour Windows, Linux et Mac. Il est très extensible, ce qui lui permet d'être utilisé à des fins très diverses, le but premier étant d'être utile aux administrateurs de réseau. Ça, c'est la version officielle. C'est un logiciel de balayage de port utilisé pour rechercher la présence de périphériques informatiques connectés à un réseau. C'est parfait pour surveiller sa propre sécurité informatique puisqu'on détecte les points faibles de notre réseau en deux coups de cuillère à pot. Mais c'est surtout sympa pour aller voir si certains ports sont ouverts chez le voisin ou qui vous voulez, dès que vous connaissez son adresse IP, ce qui est fort facile.

https://angryip.org/

Je peux lancer angryip à partir d'une adresse IP que j'encode et le soft va chercher des ports ouverts tout autour de cette adresse.

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

Lorsque la petite lumière verte s'allume, c'est que je suis tombé sur un port ouvert. Je copie/colle l'adresse IP en question et l'envoie dans la barre de recherche. Et je tombe sur la confirmation de l'abonnement internet de l'immeuble où je vis.

Mais ça c'est un peu la version coup de chance. Si je fais la même chose avec l'IP d'un site en particulier, je tomberai peut-être sur des ports ouverts. Ce qui me mènera PEUT-ÊTRE à quelque chose. Et ce quelque chose me demandera probablement un identifiant. Une caméra, un scanner, une imprimante, n'importe quoi qui est potentiellement connecté. Normalement, lors de l'installation, la personne en charge est supposé créer un mot de passe et un identifiant. Parfois la personne le fait, parfois elle se contente d'indiquer « administrateur » ou « admin » ou parfois elle laisse les identifiants par défaut de la machine.

Il y en a des milliers, selon les marques et selon les appareils.

www.routerpasswords.com/ est une base de données qui va vous lister la plupart de mot de passes par défaut. De tout appareil connecté imaginable. Encore une fois, ce site n'apporte une information conséquente que parce que des gens sont négligents. Mais tout le monde est négligent à un moment ou à un autre.

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)

Dans l'exemple ci-dessus, pour la marque de caméra de sécurité AXIS, nous avons le nom d'utilisateur et le mot de passe par défaut des différents modèles.

5. Localiser une adresse IP

Une adresse IP (avec IP pour Internet Protocol) est le numéro qui identifie chaque ordinateur connecté à Internet, ou plus généralement et précisément, l'interface avec le réseau de tout matériel informatique (routeur, imprimante) connecté à un réseau informatique utilisant l'Internet Protocol (définition Wikipédia).

Il existe différents types d'adresses IP comme les adresses IP privées, les adresses IP publiques, les adresses IP statiques et les adresses IP dynamiques.

Adresse IP privée

Une adresse IP privée est l'adresse de votre appareil connecté sur le réseau domestique ou professionnel. Si vous avez plusieurs appareils différents connectés à un seul fournisseur d'accès Internet (FAI), tous vos appareils auront une adresse IP privée unique. Cette adresse IP n'est pas accessible à partir d'appareils situés en dehors de votre réseau domestique ou professionnel.

Vous pouvez trouver l'adresse IP privée de votre appareil en utilisant quelques techniques. Si vous êtes un utilisateur Windows, il vous suffit d'aller à l'invite de commande et d'entrer la commande ipconfig. Si vous êtes un utilisateur Mac, vous devez alors entrer la commande suivante ifconfig dans votre application Terminal

Si vous utilisez l'internet sur un téléphone portable, vous pouvez aller dans vos paramètres Wifi pour trouver l'adresse IP. Les utilisateurs d'iOS peuvent trouver l'adresse IP en cliquant sur le bouton "i" à côté du réseau auquel ils sont connectés. Les utilisateurs d'Android peuvent cliquer sur le nom du réseau dans leurs paramètres Wifi, et l'adresse IP s'affichera.

Adresse IP publique. Votre adresse IP publique est la principale adresse IP à laquelle est connecté le réseau de votre domicile ou de votre entreprise. Cette adresse IP vous connecte au monde entier, et elle est unique pour tous les utilisateurs.

Adresses IP statiques et dynamiques. Toutes les adresses IP privées et publiques peuvent être statiques ou dynamiques. Les adresses IP que vous configurez manuellement et que vous fixez sur le réseau de votre appareil sont appelées adresses IP statiques. Les adresses IP statiques ne peuvent pas changer automatiquement.

L'adresse IP dynamique se configure automatiquement et attribue une adresse IP à votre réseau lorsque vous configurez le routeur avec Internet.

Lorsque vous avez l'adresse IP d'un site ou d'une personne, vous pouvez en trouver une localisation approximative.

J'utilise https://www.iplocation.net/ . Pas parce qu'il est meilleur qu'un autre, mais parce qu'il compare les résultats de plusieurs moteurs de recherche d'adresse IP. Dans mon cas, deux des quatre moteurs me localisent en Thaïlande, dans la province de Chonburi et plus précisément à Pattaya, où je réside pour le moment.

Les moteurs me donnent une latitude et une longitude que j'introduis dans Google maps.

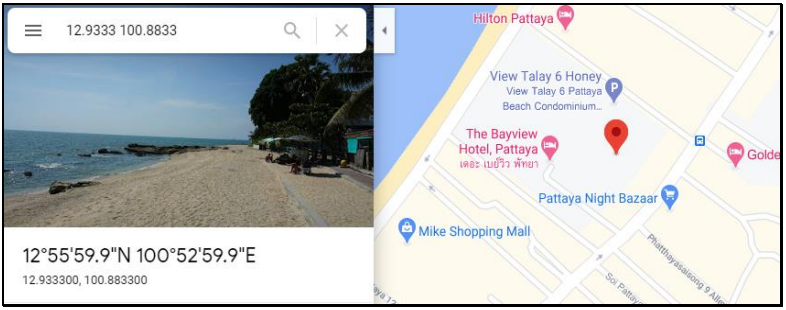
https://maps.google.com/

Ça n'est pas comme dans un film où la terrible machine de l'agent surpuissant trouve le numéro de mon appartement. Parce que je n'habite pas là où Google maps me désigne. Mais à 500 mètres de là à peu près.

La localisation de l'IP d'un site web est encore plus fastidieuse car le site peut être hébergé n'importe où, et rarement où se situe l'entreprise ou l'organisation. J'ai un

site hébergé chez one.com et quand je localise l'IP de mon entreprise, je suis perdu en Scandinavie.

Mais comme toute méthode d'investigation, celle-ci est à essayer, parce qu'elle peut donner des résultats intéressants.



6. Localiser une adresse Email

Pour retracer un mail, vous devez localiser l'en-tête du mail qui l'a accompagné. Chaque courriel a un en-tête et un corps de message. Un courrier électronique peut passer par plusieurs étapes et un en-tête est ajouté avec l'adresse IP du serveur de messagerie qui traite le courrier électronique. Lorsqu'un courrier électronique atteint sa destination finale, votre fournisseur de messagerie ajoute son adresse IP à l'en-tête. L'adresse IP du tout premier en-tête ajouté au courrier électronique est l'adresse IP du serveur de courrier électronique de l'expéditeur.

Qu'est-ce qu'un en-tête de courrier électronique ?

L'en-tête d'un courriel contient des informations sur le courriel telles que l'expéditeur, le(s) destinataire(s), le sujet, la date/heure d'arrivée, les pièces jointes et le chemin d'acheminement du courriel de l'expéditeur au destinataire. *Tous les courriels n'ont pas un en-tête de courriel approprié qui vous permet de remonter jusqu'à l'expéditeur d'origine.*

Où se trouve l'en-tête du courrier électronique ?

Pour envoyer et recevoir des courriers électroniques, nous utilisons des clients de messagerie tels qu'Outlook et Thunderbird. Avec la prolifération des fournisseurs de courrier électronique gratuits, beaucoup d'entre nous utilisent l'interface de Webmail fournie par Gmail, Yahoo et Hotmail. Chaque client et interface de Webmail offre des moyens différents pour récupérer un en-tête de courriel.

Client web Gmail

Ouvrez le message électronique dont vous voulez localiser l'en-tête. Cliquez sur la flèche vers le bas à côté du lien Répondre sur le côté droit.

Sélectionnez *Afficher l'original* pour ouvrir une fenêtre contextuelle avec l'en-tête et le corps du texte.

Client Web Yahoo

Ouvrez le message électronique dont vous voulez localiser l'en-tête du courriel. Cliquez sur la flèche vers le bas à côté du lien *Plus*. Sélectionnez *View Full Header* pour ouvrir une fenêtre popup avec l'en-tête complet.

Client Webmail Outlook

Ouvrez le message électronique dont vous voulez localiser l'en-tête. Cliquez sur les trois points (...) à côté du lien "Forward" sur le côté droit. Sélectionnez *Afficher les détails du message* pour ouvrir une fenêtre contextuelle avec l'en-tête complet.

Attention qu'un message envoyé avec une adresse Gmail n'est pas traçable via son adresse IP.

Si vous n'êtes pas trop chaud pour analyser chaque ligne d'un en-tête pour en découvrir l'adresse IP, il existe un outil qui fera ça bien plus vite que vous.

http://mxtoolbox.com/EmailHeaders.aspx

Avec https://emailrep.io/ vous saurez si une adresse email a une mauvaise réputation. Si elle a servi massivement à envoyer des spams, ou si l'adresse est blacklistée sur certains serveurs et depuis quand.

7. Trouver des informations sur l’origine d’une photo numérique

Les smartphones (et de nombreux appareils photo numériques) intègrent des coordonnées GPS dans chaque photo qu'ils prennent. Oui, les photos que vous prenez contiennent des données de localisation, du moins par défaut.

Les coordonnées GPS sont stockées sous forme de "métadonnées" intégrées dans les fichiers photos eux-mêmes. Il vous suffit de consulter les propriétés du fichier et de le rechercher.

Dans Windows, vous cliquez avec le bouton droit de la souris sur un fichier photo, sélectionnez "Propriétés", puis cliquez sur l'onglet "Détails" dans la fenêtre des propriétés. Recherchez les coordonnées de latitude et de longitude sous GPS.

J’ai pris cette photo dans une petite rue de Bangkok, le 11 novembre 2020. Les fonctions de mon téléphone, je le sais maintenant, sont activées par défaut. Ce qui signifie que les coordonnées GPS de la prise de vue ont été enregistrées. Et quand je dis « enregistrées », ça n’est pas à peu près. Quand je zoome sur la carte, j’arrive directement dans la rue en question.

Vous aurez aussi d'autres informations de moindre importance, comme la marque et le modèle de l'appareil, la date de la prise de vue, l'angle, la durée d'exposition, photo prise avec ou sans flash…

Merveilleux pour une mission de renseignement.

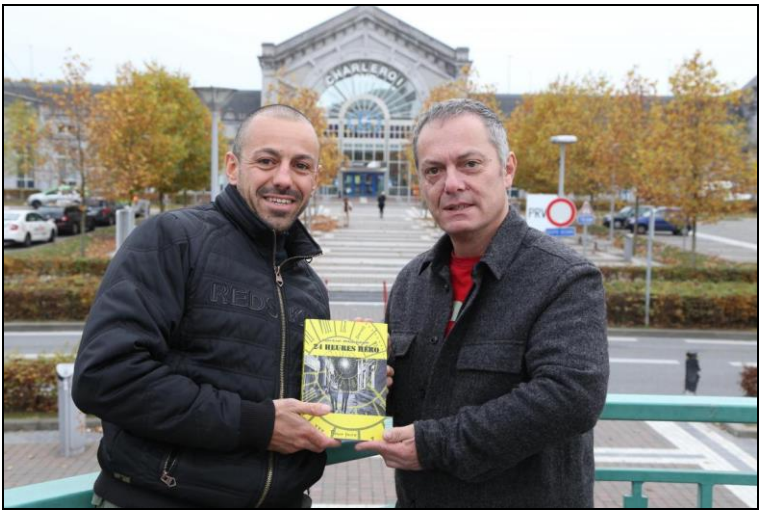
Oui, si vous avez accès à la photo originale et pas une copie. Oui, si la personne n'a pas désactivé l'enregistrement par défaut des coordonnées GPS. Quant aux photos trouvées sur les réseaux sociaux, vous ne pourrez pas les localiser car la plupart des réseaux bloquent la publication des métadonnées des photos.

8. Tracer la vie d'un individu grâce à une photo

La reconnaissance faciale et l'identification de personnes pour le grand public ne sont plus un rêve, ou un cauchemar selon les points de vue personnels. La technologie existe, vous l'avez vue dans des tas de films. Vous vous dites que c'est réservé à des agences gouvernementales pour la localisation des méchants terroristes. C'était vrai jusqu'il y a peu. Il y a une règle simple avec les outils du renseignement, et cette règle est probablement valable dans d'autres domaines : toute technologie de pointe réservée aux services de sécurité et de renseignement finira dans votre supermarché un jour ou l'autre. Si une technologie existe et qu'elle intéresse des gens, elle finira dans l'espace public. Car si une personne l'a inventée, une autre personne y parviendra. Une troisième personne la produira moins

chère. Un avantage technologique est toujours de courte durée.

La reconnaissante faciale n'échappe pas à cette règle, nous le verrons au cours de ce chapitre. Il existe bien d'autres moyens de tracer une photo et d'en obtenir de l'information. Il faut de la méthode, du travail, de l'imagination et un peu de chance.

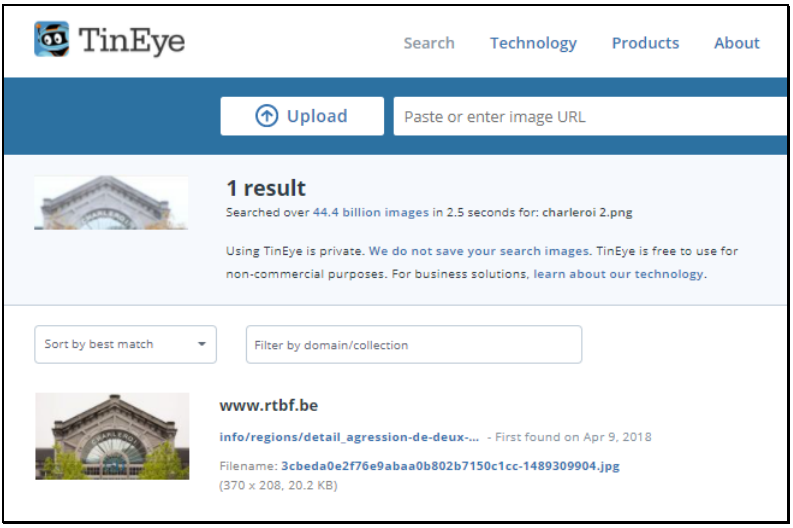


Cette photo a été prise pour la promotion d'un bouquin écrit avec mon associé et ami. Elle a été publiée dans un journal, donc si je la lance sur Google Images, pas de problème, je localise la photo.

Mais imaginons un instant que ce ne soit pas une photo publique. J'ai donc fait une capture d'écran de l'arrière-plan, là où on voit un bâtiment.

Il s'agit d'une simple capture d'écran de mauvaise qualité.

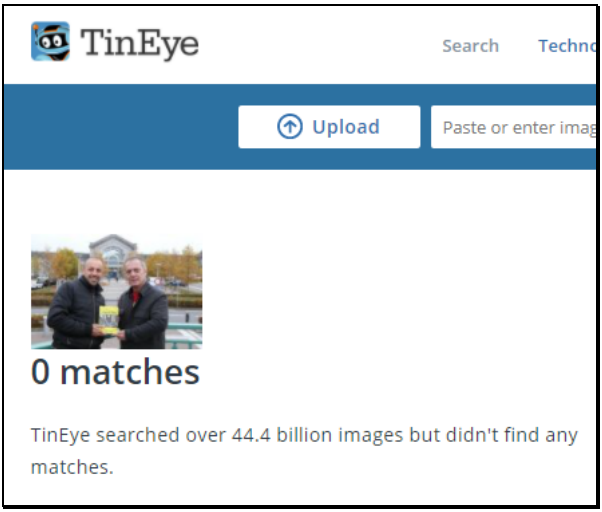
Je la lance sur Google Images, sur Bing, Yandex, et sur TinEye.



Le but initial de TinEye était de trouver d'autres tailles de la même image, et pendant de nombreuses années, il n'a fourni que cela. Ils affirment aujourd'hui détenir une base de données de deux milliards de photos et en rajouter dix millions par mois. TinEye se concentre entièrement sur la recherche d'autres utilisations de la même image. Ma capture d'écran est localisée, sans que le lien soit une photo

identique. Le moteur a simplement reconnu le bâtiment. Ce que Google ni aucun autre moteur n'a pu faire.

En revanche, lorsque je lance la photo originale sur Tineye, le moteur ne l'identifie pas.



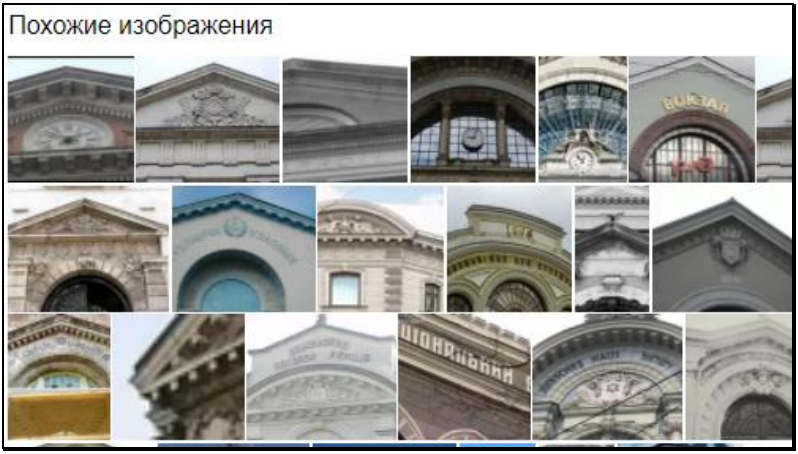
En d'autres termes, la localisation d'une photo peut se faire de façon simple si elle est dans le domaine public. Si elle ne l'est pas, à vous de chercher un détail de la photo, de l'agrandir et de le lancer sur les différents sites dont on vient de parler.

Google Images, Bing, Yandex et Tineye ont chacun leurs particularités en lien avec la recherche inversée d'images.

Google fait de son mieux pour identifier ce qu'est le sujet d'une image et non pas qui. Souvent, lorsque vous faites une recherche inversée de photos avec Google, le moteur vous retourne des réponses comme « homme » ou « fille ». Les résultats sont généralement répartis en trois sections :

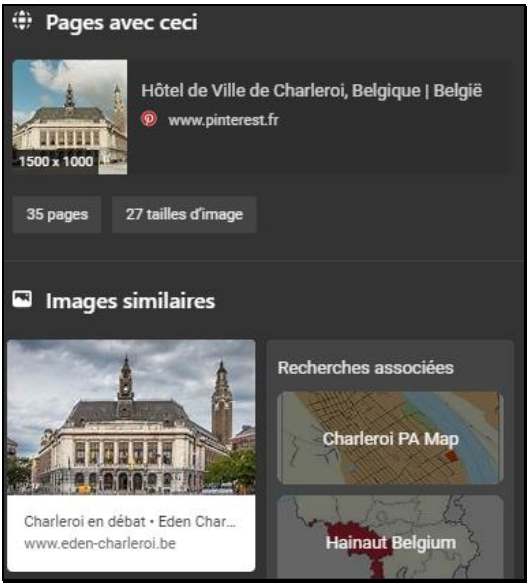
quelques résultats de recherche pour ce que l'algorithme pense être la photo, des résultats visuellement similaires (mais pas identiques) et des pages qui contiennent des images identiques. La recherche se limite également à un seul thème. Ainsi, si vous entrez une photo d'une maison située près d'un lac avec des montagnes, vous n'obtiendrez pas de photos de maisons situées près d'un lac avec des montagnes, mais uniquement des maisons visuellement similaires, sans tenir compte des lacs ou des montagnes.

Yandex est une mine d'or pour la recherche d'images inversées. Il fournit des tailles supplémentaires de la même image, des images visuellement proches, et de nombreux résultats où des images similaires figurent sur les pages. Dans notre exemple avec la gare de Charleroi, il n'a pas réussi à identifier le lieu avec précision, mais m'a proposé beaucoup d'endroits très ressemblants. On se rapproche, on se rapproche.



https://yandex.com/images/

Bing a une caractéristique unique que j'apprécie beaucoup : vous pouvez y découper des zones de votre photo et voir les résultats en direct. C'est très bien pour des images de haute qualité avec beaucoup de sujets identifiables. De plus, par rapport à Google, Bing essaie d'identifier des éléments dans une photo et de trouver des images qui contiennent tous ces éléments. Ainsi, une photo d'une voiture ancienne garée à côté d'un arbre déclenchera des correspondances qui contiennent un arbre et une voiture ancienne, alors que Google choisit un seul sujet fort et le suit. Bing se distingue également en essayant d'identifier de manière proactive les visages, les produits et d'autres éléments dans les images. Une image haute définition de plusieurs sujets célèbres mettra en évidence chacun d'entre eux. Dans le cas de la gare de Charleroi avec une mauvaise photo, Bing ne trouve rien. Par contre, quand j'utilise une photo de bonne qualité d'un bâtiment public, cela fonctionne très bien.



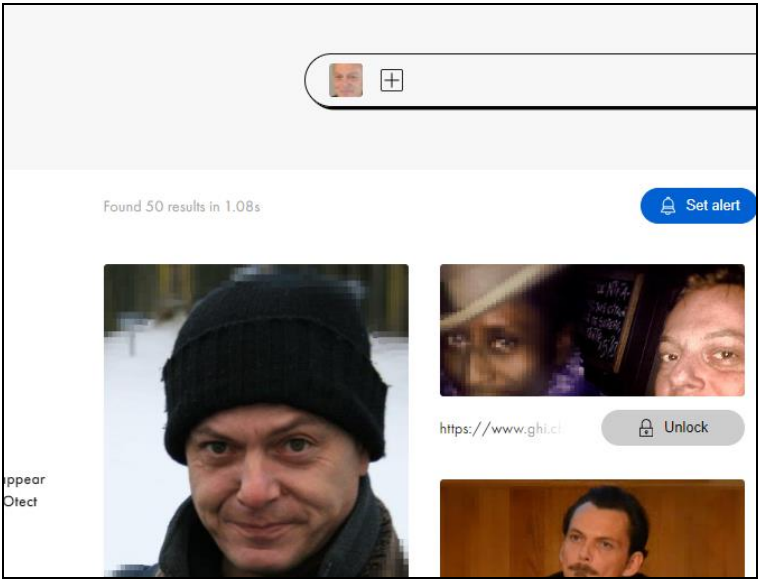
https://www.bing.com/images

Un site polonais se démarque complètement de tout ce qui existe. Avec Pimeyes, nous rentrons dans la science-fiction. Ou plutôt dans la reconnaissance faciale. Il ne s'agit donc plus de retrouver une même photo diffusée à divers endroits. Il s'agit de retrouver des photos d'une même personne.

Dans l'exemple ci-dessous, j'ai lancé dans le moteur une photo de moi prise en 2018. Quelques secondes plus tard, le site me propose toute une série d'autres photos. L'une d'entre elles est une photo de moi prise en vacances en Ecosse en 2008. Les autres photos proposées ne sont pas de moi, mais souvent très ressemblantes. Sur l'une d'elles, j'ai des doutes s'il s'agit bien de moi ou pas.

Une autre application de ce type existe en Russie, Findface. Elle équipe les caméras de sécurité de Moscou depuis 2020 et est capable d'identifier à peu près n'importe qui grâce à l'utilisation du plus grand réseau social russe. En matière de non-respect absolu de la vie privée, il va être difficile de faire mieux, mais je suis certains qu'on y arrivera.

Pimeyes permet également de soumettre plusieurs photos de la personne recherchée pour que le logiciel puisse lui envoyer une notification lorsque de nouvelles photos sont publiées en ligne.



L'outil n'est pas parfait. Il faut une photo de face, prise d'assez près. Mais il ouvre la grande porte. Le moment où il suffira de prendre la photo d'une personne en rue pour l'identifier sur les réseaux sociaux. On y est. Presque.

On peut faire des tests gratuits, mais les liens vers les photos sont cachés. L'abonnement démarre à 15 euros par mois.

https://pimeyes.com/

Une application commerciale de la recherche d'images inversées m'a été demandée par un client à la recherche du fabricant d'un produit cosmétique. Le client savait que le produit était fabriqué en Asie et souhaitait l'importer en Europe. Le nom du produit était différent d'un pays à l'autre, ce qui compliquait l'idée de remonter à la source. En lançant le nom du produit sur Google, je trouvais des tas de distributeurs, mais pas le fabricant. La plupart des distributeurs, quel que soit le produit, ne réalisent pas eux-mêmes les photos de promotion pour le marketing. Le plus souvent, ils utilisent les photos du fabricant. J'ai donc lancé des recherches avec quelques photos provenant de distributeurs et trouvé le producteur thaïlandais en quelques minutes.

Comme vous l'aurez compris, chaque moteur de recherche a ses forces et ses faiblesses. N'oubliez pas non plus qu'aucun de ces moteurs de recherche n'indexe profondément Instagram, Twitter, Facebook et d'autres médias sociaux. Il est important d'utiliser tous ces moteurs de recherche lors d'une enquête, car vous risquez fort de manquer une corrélation si vous ne le faites pas.

La recherche inversée de photos est un axe majeur de l'investigation. Pour un journaliste, cela permet de vérifier qu'une photo n'est pas utilisée dans le cadre d'un fake. Une

photo soi-disant prise durant une émeute est-elle authentique ? S'agit-il bien de la même émeute ? A la date dont on parle ? Est-ce que ça ne serait pas un évènement qui s'est déroulé ailleurs ? Pour l'enquêteur minutieux, c'est un outil formidable en recherche de personne.

9. Investigations poussées via les images satellite

Pour un enquêteur, Google earth ou Google map sont des outils indispensables aujourd'hui. Google map est un système de cartographies détaillé et Google earth contient des données 3D extrêmement précises, permettant d'explorer les rues de n'importe quelle ville dans le monde.

Dans Google Maps, vous pouvez trouver des photos en cliquant sur la section « Photos » sous la barre de recherche de carte sur le côté gauche de votre écran.

Google Street View se trouve dans Google Maps. Il contient des photographies détaillées à 360 degrés prises au niveau du sol et reliées ensemble. Cela permet à l'utilisateur de littéralement marcher dans les rues et d'identifier bâtiments, entreprises, commerces, monuments…avec une relative précision. Non, vous ne pouvez pas lire les noms à l'entrée d'un bâtiment. Pour ça, il vous faudra encore vous déplacer.

Si vous devez préparer une planque, vous avez accès à tout le quartier, via cartes ou images satellites, ce qui vous permet de préparer votre observation. Souvent, vous avez la possibilité d'aller vous balader dans le quartier grâce à l'application « street view ». Très utile quand vous devez

faire une vérification d'une entreprise et que vous constatez que l'adresse en votre possession est celle de la poste, d'un immeuble délabré ou d'un terrain vague.

Si vous devez assurer la sécurité d'un lieu, un stade par exemple, vous aurez une vue aérienne du stade, la cartographie de tout le quartier et aussi une manne de photos du stade, que ce soit de l'intérieur ou de l'extérieur.

Si votre job consiste à recueillir des informations sur une entreprise, vous pouvez en avoir une vue aérienne assez proche avec une vue plongeante sur les installations.

Mauvaise nouvelle pour les terroristes en herbe, la plupart des sites « secret défense » sont floutés. Ce qui peut se compenser via la fonction vidéo de Google. En effet, si je passe au-dessus de la centrale nucléaire de Tihange, la fonction satellitaire de Google map ne fonctionnera pas car le terrain est flouté. Mais si je tape le mot « Tihange » sur Google vidéo, je me retrouve avec énormément de matériel filmé. Pris séparément, ces films ne représentent pas un danger pour la sécurité. C'est leur nombre et la diversité des images qui le sera.

Films, vidéos, cartes et images satellites sont des outils totalement complémentaires. Et vous obtiendrez le même genre de résultats avec des tas d'endroits supposés confidentiels. Vous pouvez utiliser Google earth sans le télécharger, mais vous allez manquer des tas de fonctionnalités. Comme c'est gratuit et formidable, je vous engage vivement à le télécharger ici : https://www.google.com/earth/

Google Earth offre un certain nombre de fonctionnalités que Google Maps n'offre pas, y compris l'imagerie satellite historique et les modèles 3D du terrain et des bâtiments. Il est aussi possible de rentrer dans certains bâtiments publics.

Waze est une application de navigation et de trafic en direct qui fonctionne pour les mobiles et les tablettes avec fonctions GPS (Android et iOS). En gros, c'est un GPS, en mieux, sauf la pub qui arrive régulièrement. Les avantages de Waze, outre sa gratuité, sont que vous pouvez chercher un endroit en fonction de son adresse OU de son nom. Comme l'information arrive en temps réel, vous saurez quand changer de trajet en fonction des travaux ou d'accidents. Accessoirement, Waze vous prévient de la présence de radars ou de forces de police statiques.

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

Yandex Street View, c'est comme Google street view, mais en moins bien. Sauf si vous avez à investiguer en Russie, en Ukraine ou en Turquie. Dans ce cas, les résultats seront supérieurs. Ici, vous évoluez en même temps dans les photos à 360 degrés et sur une carte. Vraiment pratique pour anticiper la visite.

https://yandex.com/maps

Bing maps fait la même chose que la série Google, sauf qu'ici, on est chez Microsoft et que ça n'est pas la même technologie mise en œuvre. Ce qui est déjà un avantage car, qui dit technologie différente, dit résultats différents, ne fut-ce que des photos différentes provenant du même site. Quand l'un ne satisfait pas, on passe à l'autre. Bing maps a une particularité qui peut se montrer utile, c'est l'info trafic en temps réel.

https://www.bing.com/maps

Wikimapia est une plateforme cartographique open source pratique pour l'analyse de l'imagerie satellitaire car elle intègre l'imagerie de plusieurs fournisseurs (dont Google, Bing et Yahoo) et vous permet de basculer de l'un à l'autre. Vous pouvez rapidement passer d'un ensemble d'images à l'autre pour voir comment le même endroit apparaît ailleurs. Quoi qu'il s'agisse d'une entreprise privée, on parle bien de plateforme collaborative car chaque utilisateur a la possibilité d'enrichir l'expérience des autres.

https://wikimapia.org/

10. Traquer une cible en lui envoyant un lien de détection (Canary Token)

Un Canari token est un lien de suivi personnalisable, utile pour savoir qui clique sur un lien et où il est partagé. Les Canari tokens sont de plusieurs types. L'idée est de laisser des jetons sur votre réseau pour que les intrus puissent vous avertir lorsqu'ils commencent à faire des choses qu'ils ne devraient pas.

En gros, c'est le principe du pot de miel que l'on place quelque part où l'on sait que la cible va venir fourrer son nez, ou qu'on lui fait parvenir de façon à ce qu'il soit très tentant d'en sentir le doux parfum. La deuxième option est

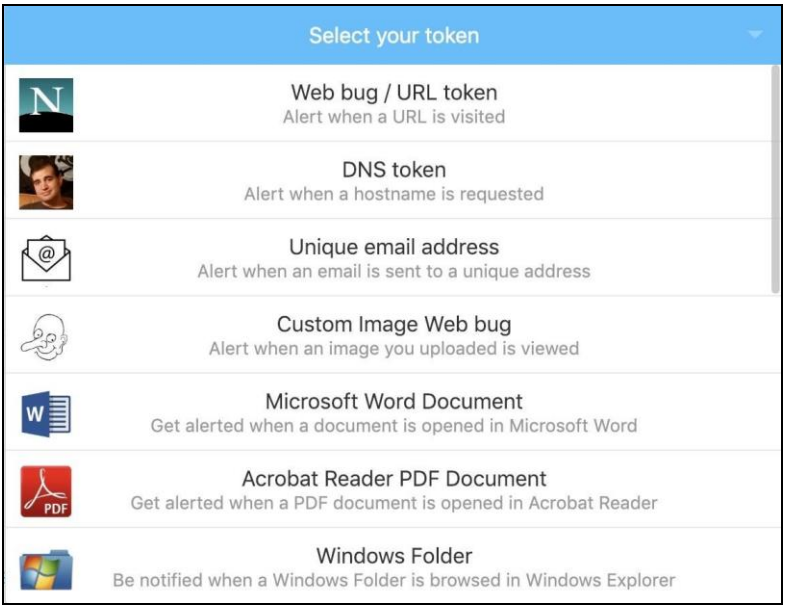
bien entendu la plus tentante. C'est exactement ce que fait le site Canary Token. Vous vous inscrivez, et le site vous génère un identifiant unique que vous pouvez alors placer sous la forme d'un lien dans un de vos emails ou toute autre forme de contact avec votre cible (pourquoi pas via whatsapp ?). Le principe du pot de miel n'est pas nouveau. Mais ce qui existait avant ce site était réservé à des gens ayant des compétences étranges utilisant des langages inconnus de la plupart des humains.

Les jetons Canary sont conçus pour être si simples que n'importe qui peut les utiliser. Selon la façon dont vous les déployez, ils peuvent détecter quand quelqu'un clique sur un lien, ouvre un e-mail, partage un fichier ou interagit d'une autre manière avec le lien de suivi.

Ce qui suit est intéressant quand vous devez localiser une personne, dans le cadre de la recherche d'un débiteur par exemple ou si votre entreprise est harcelée par un maitre chanteur. A la base, Canary Token est un outil de sécurité informatique, créé pour identifier un hacker accédant à vos données. Mais on peut l'utiliser de façon plus offensive. Attention, en finalité, nous allons trouver l'adresse IP de la cible. S'il s'agit d'une IP utilisée sur un réseau d'entreprise, vous avez une chance de le localisez avec précision. Si c'est un privé, vous trouverez au mieux la ville. S'il est protégé derrière un VPN,vous ne trouverez rien du tout.

Vous n'avez pas besoin de grand-chose pour démarrer : un navigateur et une adresse email.

Sur le site Canarytokens, vous pouvez générer un jeton Canary en cliquant sur "Select your token" et en choisissant le type que vous souhaitez créer.



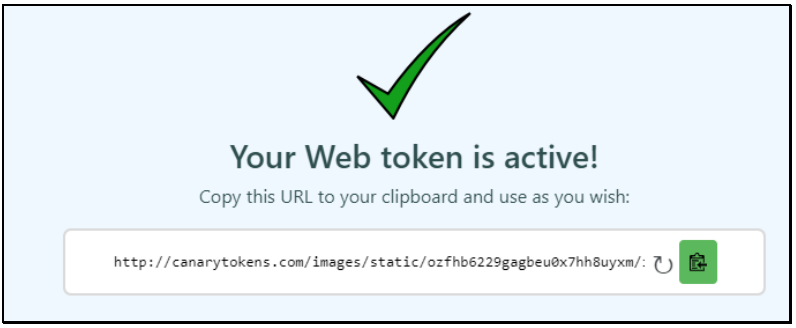
Le type de lien le plus simple à générer est un "Web bug / URL token" qui déclenchera une alerte chaque fois que quelqu'un cliquera sur le lien ou le partagera. Il s'agit d'un lien vers un site web, mais il existe également plusieurs autres options.

Un "jeton DNS" crée une alerte chaque fois qu'une URL est demandée, que la page web soit effectivement chargée ou non. Les autres jetons Canary disponibles sont des fichiers qui rendent compte de l'ouverture ou de la navigation, disponibles sous forme de documents Word, de fichiers PDF , une photo,…

Ensuite, indiquez l'adresse électronique à partir de laquelle vous souhaitez recevoir les notifications. Vous pouvez également passer cette étape et la configurer simplement via

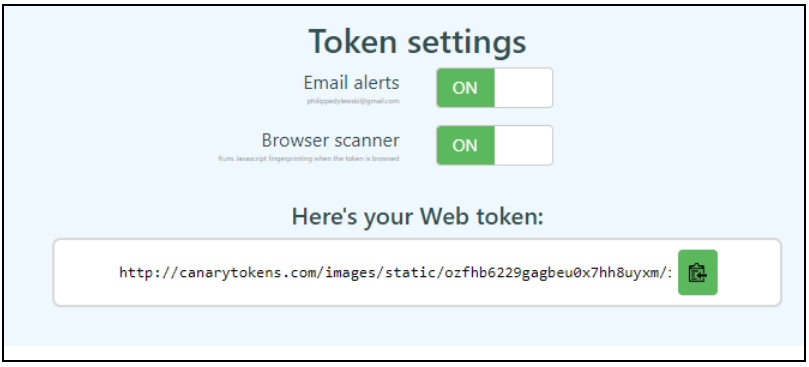
l'interface web, mais si vous perdez le lien, vous aurez beaucoup de mal à interagir avec les jetons Canary que vous aurez créé.

Puis, vous cliquez sur « create my canarytoken ».



Cliquez sur "manage this token" dans le coin supérieur droit, et vous serez dirigé vers la page qui vous permet de surveiller et de contrôler le jeton Canari.

Vous devez voir quelque chose comme ça :



Voilà, vous avez votre piège. Enfin non. Car pour piéger votre cible de façon active, il faut pouvoir lui envoyer un mail, un message par skype ou par whatsapp avec un

contenu tellement attractif que la personne voudra cliquer sur le lien.

Si vous faites un test en lançant le token via votre navigateur, vous verrez juste une page blanche, c'est normal.

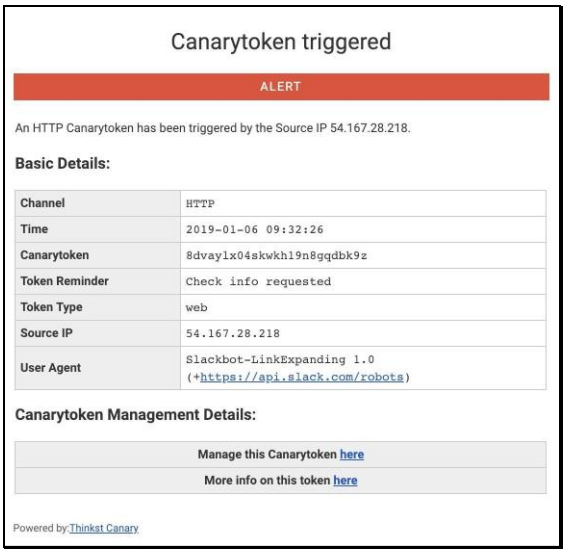
Je vous suggère d'utiliser un VPN (cf le chapitre consacré au VPN) avant de vous lancer. Cela vous évitera les retours de flamme de la part de votre cible.

Une autre façon d'utiliser un jeton Canary est de le raccourcir avec un raccourci d'URL. Vous pouvez utiliser des services comme Bit.ly pour masquer l'URL réelle. Cela vous permet de créer un token plus petit et surtout moins suspect.

https://bitly.com/

Après avoir ajouté le lien de votre jeton Canary à Bit.ly, vous pouvez utiliser le lien raccourci de la même manière que vous utiliseriez l'original. Souvent, ce lien raccourci attirera moins de soupçons que l'URL super-longue du jeton Canary.

Dès que votre piège fonctionne, vous recevez ceci :



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

L'information intéressante se trouve dans « source IP ». Il vous reste à rentrer l'adresse dans un localisateur d'adresse IP, ce que nous avons vu dans un autre chapitre.

Et si ça n'a pas fonctionné, que votre piège ne s'est pas refermé, il vous reste le loisir d'affiner votre méthode en utilisant d'autres jetons, avec d'autres types de fichiers. Cela vous demandera un peu de travail, un peu d'étude, mais rien qui demande un Bac + 12 en informatique. Si je vous propose Canarytokens, c'est parce que c'est un outil accessible au plus grand nombre. Vous pouvez commettre des erreurs, mais vous comprendrez. Vous trouverez sur le site et un peu partout sur le net, des recommandations pour utiliser au mieux les performances de ce site. Mais vous pouvez commencer à vous entrainer avec vos proches, histoire de vous faire la main.

https://canarytokens.org/

IV. Les techniques et outils de Sourcing de candidats

J'ai créé et dirigé un cabinet de recrutement pendant 15 ans. Ce que j'aimais le plus dans le job, c'était chercher les candidats. Je trouvais les interviews rasoirs la plupart du temps et dès que j'ai pu, j'ai délégué cette tache à l'équipe. Tout le monde était content puisque c'était le boss qui se tapait justement le boulot que personne ne voulait faire. Plus tard, j'ai eu un déclic : mon choix d'être « chasseur de tête » devait être pris dans un sens plus terre à terre et j'ai tout vendu pour devenir détective privé, très actif dans la recherche de personnes disparues. J'étais enfin un vrai chasseur de têtes. Ce qui ne m'a pas empêché de garder un pied dans le recrutement en proposant justement des activités de Sourcing de candidats et de vérification de CV (backgroundcheck).

Quelle que soit la situation économique d'un pays ou d'une région, trouver des bons candidats n'est jamais facile. Car à moins que vous ne soyez dans un métier unique, le candidat que vous trouverez intéressant sera aussi trouvé intéressant par les autres recruteurs. Ce chapitre s'adresse aux recruteurs professionnels tout comme à ceux qui font du recrutement de façon occasionnelle. Il est centré exclusivement sur la recherche de candidats via des techniques et des outils. Mais si votre job n'est pas lié au recrutement, ce chapitre pourra quand même vous intéresser car les techniques vues ici, peuvent être combinées avec d'autres types de missions.

1. Trouver des Emails de candidats LinkedIn

Théoriquement, il n'est plus possible d'exporter les adresses emails de vos contacts LinkedIn. C'était une bien belle fonction, mais elle a disparu. Notre intelligence se définissant grandement au regard de nos capacités à nous adapter, voyons ce qu'il est possible de faire.

Contactout est un outil de scraping d'adresses emails. En bref, ContactOut est capable de trouver instantanément l'adresse électronique et le numéro de téléphone personnels de candidats potentiels sur LinkedIn en effectuant une recherche automatique sur d'autres sites de médias sociaux et sur le web en général à l'aide d'un moteur d'intelligence artificielle. Il ne tombe pas dans le piège des autres outils de scraping LinkedIn qui passent leur temps à essayer de contourner la sécurité du site. Quand ils y arrivent, c'est en général pour quelques jours ou quelques semaines. Contactout est une extension pour Chrome. Vous devez donc l'installer sur votre ordinateur. Contactout promet une totale vérification des mails proposés. La seule chose que je crains, c'est que ça ne dure pas. Contactout est quasi unanimement considéré comme le numéro 1 de sa catégorie.

https://contactout.com/

AeroLeads est un bon outil pour générer des leads ou des candidatures avec une très bonne précision. C'est un outil polyvalent - contrairement à d'autres outils qui ne peuvent que trouver des e-mails ou simplement ajouter des leads dans les bases de données CRM. Sur votre tableau de bord Aeroleads, vous pouvez trouver le candidat ajouté avec son

nom, son titre et son employeur. En plus de cela, vous pouvez trouver l'email et le numéro de téléphone du candidat.

Vous pouvez tester Aeroleads et si l'outil fait votre bonheur, il vous en coutera un minimum de 49 dollars par mois pour une base de 1.000 prospects/candidats.

Il s'agit d'une extension Chrome qui scrape directement sur LinkedIn via votre compte. Pas de danger pour votre compte, mais n'imaginez pas des centaines de candidats par jour. Il faudra respecter les règles de sécurité de LinkedIn. Aeroleads n'est pas le premier outil du genre, loin de là. J'en ai utilisé des tas, que ce soit pour la prospection ou pour le recrutement. Ce qui distingue surtout Aerloleads des autres, c'est qu'il est toujours là. Car LinkedIn n'aime pas du tout ces scrapers et la plupart disparaissent après avoir prouvé leur efficacité.

https://aeroleads.com/

2. Automatiser la recherche sur LinkedIn ? Les limites de LinkedIn et comment les contourner

La recherche et le contact de candidats potentiels sur LinkedIn n'est pas une activité très ludique. Difficile de le dire autrement. Je parle de recherche active, celle où vous cherchez le contact. Je ne dis pas que chercher à *attirer* les candidats soit une mauvaise méthode, mais parfois elle ne suffit pas. Si personne ne vient à vous, il vous faut alors y aller.

Une fois que j'ai une liste de candidats potentiels, je leurs envoie une invitation SANS message. Cela va beaucoup plus vite et c'est bien plus efficace. Cette méthode, si vous avez un profil à peu près correct, vous ramènera plus ou moins 30% d'acceptation. C'est à ces personnes que vous envoyez un message. Car si vous faites une demande d'acceptation avec message, beaucoup de gens accepteront votre invitation sans prêter attention à votre message et je trouve embarrassant d'envoyer deux fois le même message.

Vous envisagez d'automatiser certains processus de génération de prospects sur LinkedIn ? Lisez d'abord ceci, sinon nous déclinons toute responsabilité pour ce qui pourrait arriver à votre karma.

Pourquoi ne puis-je pas me connecter à un million de personnes en 5 minutes ?

D'une part, LinkedIn rassemble, héberge, protège et organise nos données afin que ce soit le meilleur endroit pour que les professionnels se rencontrent, échangent, apprennent et travaillent ensemble. Ils font un excellent travail et sont utiles à des centaines de millions de personnes dans le monde entier. Bravo ! Mais d'un autre côté, les données qui se trouvent sur LinkedIn sont VOS données, NOS données, et LinkedIn ne serait rien sans elles. Ainsi, faire payer des centaines ou des milliers d'euros par an, pour que chacun puisse accéder aux données de ses pairs est un prix élevé lorsque vous donnez vos données gratuitement. Ok que LinkedIn mette des garde-fous. C'est normal. Si LinkedIn devenait le kibboutz de l'info, ce serait un peu le désordre et sans doute la fin de leur modèle économique. Souvent je suis d'accord que les règles

existent, tant qu'elles ne s'appliquent pas à moi ou que je peux trouver un moyen pour ne pas les respecter.

D'abord, entrons dans la tête de LinkedIn : Que veulent-ils ? De vraies personnes, qui leur donnent de vraies informations, qui les tiennent à jour, et accessoirement qui deviennent des utilisateurs payants, ce qui est leur but.

Plus ils auront ce qu'ils veulent, plus ils récompenseront les utilisateurs en leur donnant une plus grande visibilité et un meilleur accès à l'information.

Ainsi, par exemple, un tout nouveau compte avec 0 connexion, pas d'école, pas d'entreprise, pas de photo, etc. ne pourra pas envoyer autant de demandes de connexion qu'un compte vieux de 10 ans avec des milliers de contacts et 2 heures de connexion par jour.

Voici une liste (incomplète) de facteurs qui auront un impact sur vos propres limites d'action :

- Si vous avez un abonnement payant. Critère très important car virer un mendiant n'est pas pareil que bloquer un bon client bien gras.

- Date de création du profil.

- richesse du profil.

- Nombre de connexions.

- Temps passé par jour sur LinkedIn.

- Nombre de messages envoyés par jour.

- Montant des invitations en attente. Le moins possible, c'est mieux. Au-delà de 1.000, vous êtes suspect de spamming, le crime absolu.

- Combien d'articles et de publications vous publiez.

- Combien de commentaires ou d'appréciations vous donnez.

Quelles sont les limites avant de se faire taper sur les doigts ?

50 invitations par jour pour un nouveau compte gratuit.

100 invitations par jour pour un ancien compte gratuit.

350 invitations par jour pour un compte payant Sales Navigator.

Le nombre de messages que vous pouvez envoyer ira de 100 à 400 par jour en fonction de votre statut aux yeux de LinkedIn.

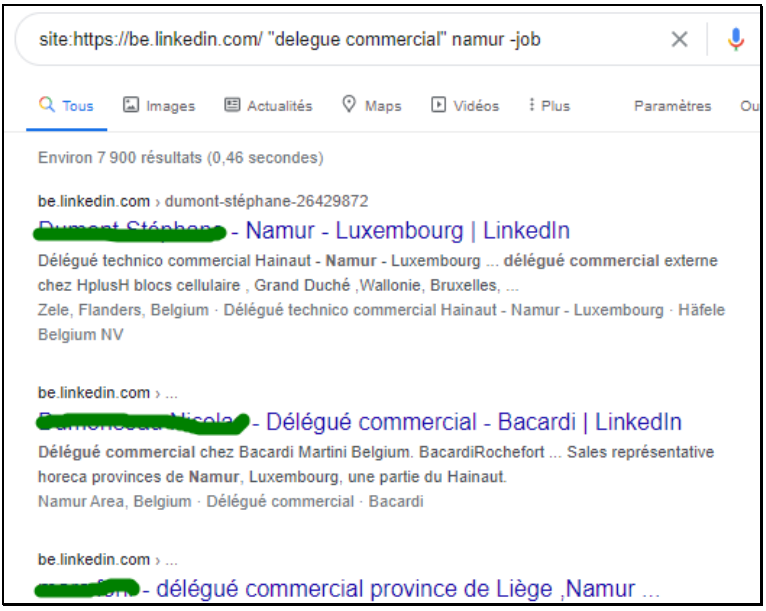
LinkedIn affirme qu'en cas de dépassement, votre compte peut être supprimé. C'est possible, mais s'ils ne l'ont pas fait avec moi, c'est qu'on peut repousser les limites d'utilisation. Quand j'utilisais un compte gratuit, j'ai été régulièrement bloqué pour plusieurs jours. Cela tient autant aux limites d'utilisation qu'aux personnes que je contacte. Si beaucoup de personnes contactées déclarent ne pas vous connaître, vous risquez d'être bloqué rapidement. Dans le cadre du recrutement, c'est beaucoup moins probable que dans le cas d'une prospection à froid. En tant que recruteur, vous êtes beaucoup moins exposé à ce problème qu'un

commercial. Il est rare qu'une personne se sente agressée en recevant une offre d'emploi, alors que ça peut se produire lorsque quelqu'un vous prospecte.

Comment contourner les limites d'utilisation ?

Si votre recherche est ponctuelle et que vous êtes pauvre, vous pouvez souscrire à un abonnement prémium, avec essai gratuit pour un mois. Quitte à ne rien payer, prenez l'abonnement qui vous offre un accès à un nombre illimité de profils. Deux ou trois jours avant la fin de votre essai, annulez l'abonnement et votre carte de crédit ne sera pas débitée. LinkedIn est à ce sujet d'une honnêteté irréprochable. La méthode est un peu mesquine si c'est pour gagner quelques sous. Elle l'est beaucoup moins si votre souhait est de tester intégralement un service avant de payer car la version d'essai gratuite vous donne accès à toutes les fonctionnalités.

Une autre méthode, qui elle vous donne un accès illimité et gratuit à LinkedIn, est la recherche booléenne via Google, que nous avons vue dans d'autres chapitres. Comme toutes les données de LinkedIn sont indexées dans Google, vous pouvez faire autant de recherche de profils que vous voulez. Aucune limite.



Cette méthode fonctionne extrêmement bien. Remarquez qu'ici j'ai fait une recherche de délégué commercial sur la région de Namur en Belgique. Constatant que je recevais surtout des offres d'emploi, j'ai recommencé la recherche en indiquant dans ma requête que je n'en voulais pas (« -job »). Si la méthode est gratuite et d'une grande finesse, elle vous demandera d'accéder à un bon niveau de compétences en recherche booléenne. Mais bonne nouvelle, nous avons vu dans un autre chapitre, qu'il existait des moteurs de recherche booléenne visant exclusivement Linkedin.

Si vous voulez absolument automatiser certaines tâches sur LinkedIn, vous avez le choix. Il y en a des centaines. La plupart sont des extensions pour Chrome. Pour moi, elles ont toutes le même point négatif, mais c'est personnel : les

extensions qui survivent aux foudres de LinkedIn sont celles qui respectent les limites d'utilisation à la lettre. Je n'aime pas les limites.

Si vous voulez automatiser votre activité sur LinkedIn, Dux-Soup est le moyen le plus efficace. En utilisant une simple extension Chrome, vous pouvez automatiser le processus d'envoi de messages personnalisés aux candidats, le suivi avec des réponses automatisées, l'approbation des connexions et le suivi des profils. De plus, vous pouvez intégrer une grande partie de cette activité à votre CRM.

Malgré son nom bizarre, Dux Soup a été l'un des premiers outils de génération de prospects LinkedIn que j'ai utilisé. Malheureusement, comme beaucoup de choses dans la vie, Dux Soup est à utiliser avec modération lorsqu'il s'agit de tirer parti de ses puissants outils. « Modération » n'est pas précisément un mot que j'affectionne.

Dux Soup peut être téléchargé gratuitement. La plupart des fonctions utiles sont payantes et peuvent être achetées par le biais d'un abonnement mensuel ou annuel. Cette extension de Chrome vous aide à mettre votre génération de candidats sur pilote automatique en automatisant des tâches telles que l'affichage de profils, l'envoi d'invitations et de messages.

Maintenant, un mot d'avertissement. Cet outil est considéré comme une "tricherie" aux yeux de LinkedIn. Si vous utilisez cet outil à mauvais escient et que vous augmentez trop les paramètres, vous pourriez recevoir un mail d'avertissement, voire voir votre compte suspendu. L'utilisation de Dux Soup prend un peu de temps, surtout quand, comme moi, vous n'êtes pas un super fan de

technologies et que vous voulez utilisez les paramètres avancés de l’extension.

Combien de temps Dux Soup va-t-il durer ? Dux Soup viole directement les conditions de service de LinkedIn, et cela pourrait signifier qu'il pourrait disparaître demain. LinkedIn pourrait tenter de poursuivre Dux Soup, ou plus vraisemblablement, sortir une mise à jour d'algorithmes qui casse ou désactive des fonctions dans Dux Soup. Il en résulte un jeu du chat et de la souris entre les deux sociétés, où l'une casse une fonction, et l'autre la répare aussi vite que possible.

Bien que cela ne se soit pas encore produit de manière significative, cela pourrait se produire. Il est donc important que si vous recherchez un outil LinkedIn solide comme le roc, ce n'est pas celui-là. Mais pour être juste, aucun outil d'automatisation LinkedIn ne le sera. C'est simplement le risque que nous prenons lorsque nous utilisons certains outils pour aller de l'avant. Bien que LinkedIn déclare officiellement que l'automatisation est contraire à sa politique, il réalise qu'une grande partie de sa base d'utilisateurs le fait. Je pense que LinkedIn ferme les yeux sur la plupart des automatisations, tant qu'ils ne sont pas excessifs ou spammeurs. Si LinkedIn le voulait, je pense qu'ils pourraient écrire un programme pour détecter la présence de plugins d'automatisation, mais ils ne le font pas.

Prix à partir de 15 dollars. Je vous suggère de ne jamais prendre l’abonnement annuel car vous ne pouvez pas être certain que l’outil sera encore fonctionnel la semaine prochaine.

https://www.dux-soup.com/

Un concurrent sérieux de Dux Soup est Prospectin, qui lui est français et sensiblement dans la même zone tarifaire.

https://www.prospectin.fr/

3. Trouver des Emails de personnes travaillant dans l'entreprise que vous ciblez

Ciblez une entreprise et obtenir un maximum d'adresses email de collaborateurs, c'est possible avec Hunter. Simple d'utilisation, vous tapez le nom d'une entreprise et vous recevez en quelques secondes les adresses email de gens travaillant dans cette entreprise. Par exemple, pour la promotion de ce livre, je vais envoyer un mail à un maximum de journalistes. Pourquoi pas ceux du Monde ?

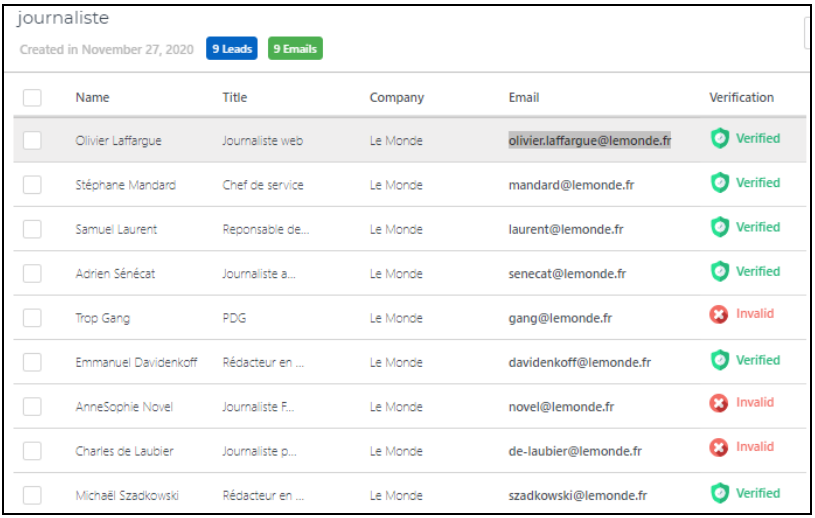
Hunter m'en propose 331. Est-ce que ce sont tous des journalistes ? Les adresses sont-elles toutes actives ? Non. Mais en plus de la liste d'adresses, Hunter me fournit les liens qui ont permis de les trouver. Ce qui veut dire que si

un lien ne correspond pas à ma recherche ou que j'estime que les liens sont trop vieux, je peux détruire l'adresse. Et ensuite, je peux exporter les résultats en format csv. La version gratuite me permet de faire 50 recherches par mois, mais je n'ai accès qu'à 10 emails par recherche. Le premier prix est à 49 dollars par mois.

https://hunter.io/

https://email-format.com fait le même job que Hunter. En gratuit et en moins bien car les adresses proposées sentent un peu le poisson.

Skrapp va chasser l'e-mail sur LinkedIn et ramène l'information de façon très structurée. En plus, une offre gratuite à 150 adresses par mois. Et un vérificateur d'adresse. Je ne sais pas comment ils font, mais le résultat y est.



https://skrapp.io/

Si vous êtes le pique-assiette du renseignement, vous pouvez faire le tour des aspirateurs d'emails et cumuler les abonnements gratuits.

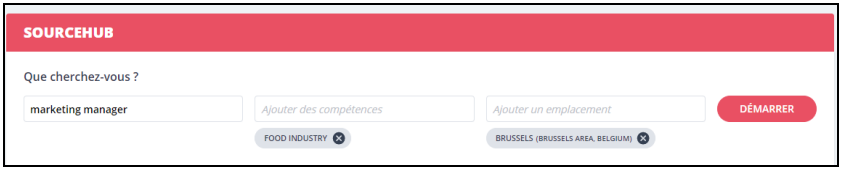
4.Trouver des candidats sur Linkedin en passant par Google

Si vous avez du mal à maîtriser l'utilisation des outils booléens, vous allez adorer SourceHub.

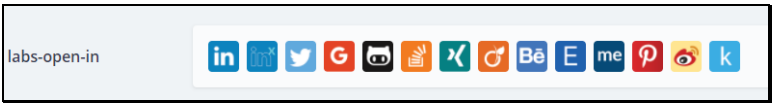
SourceHub vous évite d'avoir à utiliser les codes booléens, en mettant en place des taxonomies pour effectuer des recherches complètes pour vous, à partir de très peu de données. SourceHub vous permet de lancer votre recherche sur LinkedIn, Twitter, Facebook…En tout, 15 reseaux. Il vous suffit d'entrer le titre du poste que vous cherchez à pourvoir, les compétences que le candidat doit posséder et l'endroit où vous le recherchez.

Pas de AND, OR ou NOT. Dites simplement à SourceHub ce que vous recherchez exactement, en termes simples, et il fera le travail pour vous. Vous pouvez aussi exclure des termes de votre recherche.

Remplissez les champs avec les critères/lieux avec lesquels vous recherchez des candidats :

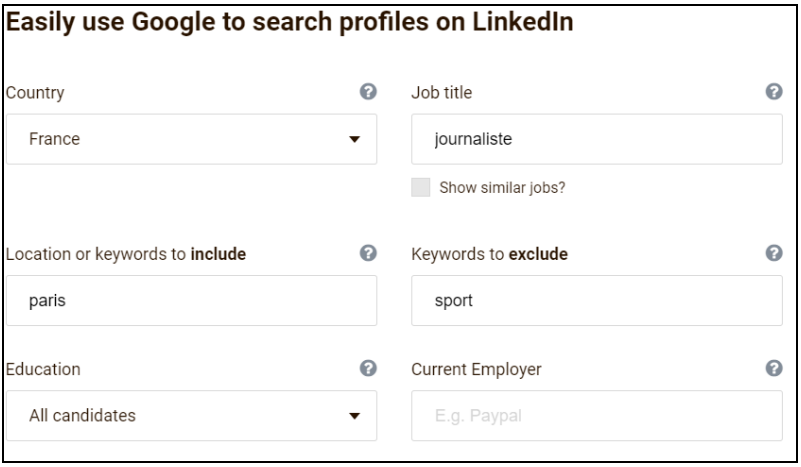


Le petit stress, c'est qu'il faut savoir que pour lancer la recherche, il faut aller dans le bas de la page et cliquer sur le réseau qui vous intéresse. Mention spéciale pour la recherche sur le web car elle vous permet de trouver les profils de candidats qui ont créés un mini-site pour exposer leur candidature, et il y en a de plus en plus.



https://source.socialtalent.com/

Recruitem est un outil gratuit qui vous permet de chasser sur Linkedin sans passer par Linkedin. Le moteur utilise la recherche booléenne avec une série de critères de votre choix et vous propose une série de profils trouvés sur Linkedin.



Ici, je cherche des journalistes parisiens en excluant ceux qui travaillent dans le domaine du sport. Simple et parfait.

https://recruitin.net/

Recruitmentgeek fait le même boulot, c'est gratuit aussi. Le moteur de recherche est moins précis, mais c'est vraiment pour faire le difficile car les deux outils sont supers et gratuits !

https://recruitmentgeek.com/

5.Rechercher des candidats sur Linkedin avec un compte gratuit

Je pars du principe que vous connaissez l'existence de Linkedin, que vous avez un compte et que vous avez une connaissance minimum du site.

Vous savez qu'il y a une barre de recherche et que quand vous lancez une recherche, un « sales manager » par exemple, vous allez avoir une collection impressionnante, et donc inutilisable, de résultats.

Je pars aussi du principe que vous savez que le premier tri des résultats, une fois que la recherche de votre futur « sales manager » est revenue avec des milliers de résultats, se fait avec la barre au-dessus de l'écran. Vous pouvez faire un premier tri si vous cherchez des gens étant ou ayant été sales managers, des offres d'emploi pour sales managers, du

contenu où vous pouvez lire des articles liés aux termes recherchés, des groupes de sales management…

C'est le basique du basique. Je n'explique pas. Si vous êtes totalement néophyte en matière de Linkedinerie, vous comprendrez le court paragraphe précédent en faisant des essais par vous-mêmes en un quart d'heure. Comme nous sommes dans le cadre d'une mission de sourcing, c'est bien sûr sur le bouton « personnes » que vous cliquez. Avoir des milliers de résultats est à peu près aussi désespérant que de n'en avoir aucun.

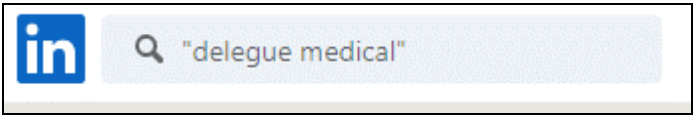
Vous pouvez commencer à limiter la recherche avec des critères de bases comme la localisation géographique, le nom des entreprises actuelles et passées, le secteur d'activité, l'école où votre candidat serait bienvenu d'être diplomé… Linkedin vous propose aussi de choisir le niveau de relation que vous avez avec les gens que vous êtes susceptible de contacter. Dans le cadre d'un sourcing candidats, que les gens soient de premier niveau (déjà dans vos relations) ou dans les relations de vos relations, est plutôt sans grand intérêt.

Linkedin et la recherche booléenne

Le moteur de Linkedin fonctionne comme celui de Google. Un chapitre précédent est consacré aux recherches booléennes. Ce que je vais faire ici, c'est donner des exemples d'application.

Je suis à la recherche d'un délégué médical pour la région de Bruxelles. Mon client souhaite rencontrer des candidats qui ont une expérience probante dans un job similaire.

Le premier niveau de tri en recherche booléennes sera l'utilisation des guillemets. Par exemple, si je cherche *délégué medical*, j'obtiens 318.000 résultats. Parce que Linkedin me renvoie les délégués médicaux, les délégués de toute obédience et toute personne ayant le mot « médical » dans son profil. Oui, ça fait du monde. Et encore, je ne simule pas une recherche où se trouvent des termes anglophones, ce qui multiplierait les résultats de façon astronomique. Sauf que bien sûr, vous avez déjà pris soin de limiter vos recherches à une zone géographique bien précise.



Je me retrouve avec 166 profils.

Mais comme je suis très respectueux de la diversité, je suis totalement indifférent du fait que les candidats soient des hommes ou des femmes. Pour tous les autres genres, LinkedIn n'a encore rien prévu. Je vais alors utiliser la fonction « OR » qui me permet en une seule recherche, de valider toutes mes options.

Ce qui me donne 437 résultats. C'est trop. Mais surtout, mon client veut des candidats avec une expérience de la délégation médicale mais uniquement ceux qui ont

l'habitude de visiter des médecins. Il ne veut pas de ceux qui visitent les pharmacies car c'est un profil différent.

"delegue medical"OR"deleguee medicale"NOT"pharmacie" NOT"pharmaceutique"

Ici, avec le terme « NOT », j'exclus ceux qui ont le mot « pharmacie » dans leur profil et il ne me reste plus que 411 liens. Pour les recherches complexes, qui combinent des séries de critères, il vaudrait mieux utiliser les parenthèses, qui aident à la structuration de la recherche.

("delegue medical"OR"deleguee medicale")NOT("pharmacie"OR"pharmaceutique")

Ici, j'exclus les candidatures qui contiennent soit le mot "pharmacie » soit le mot « pharmaceutique ».

Je n'ai plus alors que 174 profils.

Comme vous pouvez le constater, le niveau de connaissances techniques pour utiliser la recherche booléenne sur LinkedIn est plutôt bas. Ce qui rend son utilisation complexe, c'est la capacité à structurer sa pensée et sa recherche pour les transformer en signes. Un tout petit peu d'entrainement, et vous serez un prince de la traque.

V. Le matériel d'espionnage

Comme vous, j'ai grandi avec les films d'espionnage. Fasciné par le charisme, le courage et le charme de ces héros. Et aussi par le pouvoir que donne le matériel qu'ils utilisent. L'ironie de l'histoire, c'est que le matériel utilisé par ces agents jusqu'à la fin du XXème siècle se retrouve en vente sur Amazon pour quelques euros.

J'ai démarré ma carrière de détective privé en 2004. Pour donner un exemple, un tracker GPS faisait la taille d'une boite à chaussures et coutait une fortune. Bien entendu, il existe toujours des prestations réservées aux services d'états. Le commun des mortels n'y a normalement pas accès. Nous ne pouvons pas localiser un ordinateur d'un simple clic et une simple photo prise dans la rue ne nous permettra pas de savoir où habite la personne ni ce qu'elle a mangé au petit déjeuner. Les films ont toujours une longueur d'avance sur nous. Cette longueur d'avance est de plus en plus courte.

L'utilisation de tous les outils dévoilés ici est totalement illégale lorsqu'il s'agit d'obtenir à son insu des renseignements sur une personne ou une organisation. Vous le savez déjà. Toutes les techniques présentées dans ce livre ont une finalité industrielle ou commerciale et la plupart de ceux qui utiliseront le matériel présenté ici, le feront pour espionner conjoint et enfants. Si j'étais dans le jugement, j'écrirais d'autres choses.

Je ne présente ici qu'un ou deux produits par catégorie. Parfois aucun et alors j'énumère les critères d'achat. Parce que sinon, ce livre ferait la taille de l'Encyclopédie

Universalis. De préférence, les meilleurs ou en tout cas les meilleurs pour un prix raisonnable. Le matériel coutant plus de quelques centaines d'euros n'est pas présenté ici. J'explique aussi les points forts et faibles du produit. En fin de chapitre, vous trouverez quelques liens vers des sites où vous pouvez acheter le matériel. Enfin, j'insiste sur les arnaques, plutôt rares avec le matériel, et sur les limites d'utilisation, qui sont souvent oubliées par les fabricants.

1.Espionner un téléphone à distance

Le rêve total de l'agent de renseignement. Prendre le contrôle d'un téléphone portable à distance. Première question : est-ce vraiment possible ou bien est-ce une arnaque doublée d'une légende ? C'est possible. Mais avec des conditions telles que son usage dans la pratique est très limité. Une technique coûteuse vous est expliquée au paragraphe 19.

La première contrainte est que vous devez avoir un accès physique au téléphone et que vous en connaissiez le code d'ouverture. Et une dizaine de minutes pour installer le logiciel. Tous ceux qui vous promettent un accès à distance mentent, même ceux qui affirment qu'il est possible de le faire via une connexion Bluetooth, car elle sera probablement détectée par le téléphone ciblé.

Avant tout achat, vérifiez que votre futur logiciel est compatible Mac ou Pc, Android ou iOS, en fonction de votre matériel.

Les fonctionnalités de base sont l'enregistreur de frappe, la capture d'écran à distance, l'accès aux photos et aux vidéos, l'accès à toutes les messageries et accès aux comptes de réseaux sociaux de la cible et bien sûr, la géolocalisation en temps réel. Ça, ce sont les fonctions légales en Europe.

En Europe, il est interdit d'utiliser des logiciels qui contrôlent micro, caméra et logiciels de messagerie. Mais aucun problème pour acheter le matériel facilement.

Flexispy est l'une des applications téléphoniques d'espionnage les plus avancées au monde. Elle vous permet de suivre les SMS, Facebook, WhatsApp, Twitter et de localiser les appareils. Elle est compatible avec Android, iOS, PC et iPad.

Elle est disponible en version lite, premium et extrême. Toutes ont des caractéristiques différentes. Une fois installé, il permet de suivre les journaux d'appels et autres activités du téléphone ciblé. Pour consulter le rapport d'activité, il vous suffit de vous connecter au compte Flexispy.

L'outil n'est pas donné. Mais il est le meilleur et il est quand même abordable. Budget entre 35 et 250 euros par mois.

https://www.flexispy.com/fr/

2. Le stylo espion

Comme son nom l'indique, il s'agit d'un authentique stylo qui a pour mission de filmer et/ou d'enregistrer une situation.

Pour mériter ce titre, le stylo doit :

- Ecrire. Je sais, cela semble une évidence, mais apparemment pas pour tous les fabricants.
- Enregistrer le son ou filmer avec un niveau de qualité acceptable. Oubliez la top qualité.
- Ressembler à un vrai stylo et donc être indétectable à l'œil.
- Avoir une autonomie suffisante et une bonne capacité de recharge.

Le stylo caméra espion de SIRGAWAIN fait tout ça très bien pour un budget de 50 euros.

L'outil est fort bien, cela ne veut pas dire qu'il soit parfait. Vous devez filmer à proximité de votre cible et dans un environnement lumineux. Il faut impérativement une carte mémoire, qui n'est pas fournie. Il n'y a pas non plus d'outil de stabilisation de l'image, ce qui fait que si vous filmez en mouvement, le résultat sera mauvais. Enfin, la caméra n'enregistre pas le son, mais c'est un standard sur ce type de produit.

3. Le drone avec caméra

Inutile d'expliquer ce qu'est un drone, c'est un truc qui ressemble à un jouet pour gosses, avec le design d'une araignée sans les poils et qui permet de survoler une cible en vol statique.

Evidemment, surveiller une cible depuis un hélicoptère, c'est quand même autre chose question adrénaline, mais quand on sait qu'un drone s'achète à partir de 20 euros, cela mérite une certaine réflexion.

Si vous voulez acheter un drone pour vos activités de renseignement, il est indispensable d'être attentif à quelques éléments :

- La première chose, c'est que le drone soit équipé d'une caméra

- Contrôlable à une distance respectable. Si vous voulez observer les mouvements de marchandises de votre concurrent, il serait tout de même dérisoire de devoir le faire à partir de son parking. L'autre raison pour laquelle ce critère est crucial est que si votre drone a une faible portée, vous devrez le faire voler à une altitude où il sera immédiatement détecté. Soyons clair, un drone n'est pas un satellite et est plutôt difficile à rendre discret sauf si vous décidez d'investir dans des machines à plusieurs centaines de milliers d'euros mais qui n'ont pas leur place ici.
- La qualité de l'image ET la stabilisation de l'image
- L'autonomie
- La vitesse peut être un critère, mais dans les missions de renseignement, je n'en vois pas trop l'utilité.

Ici, en raison de la grande diversité de prix, je vais vous parler de deux produits. Je n'en ai utilisé aucun des deux, j'ai seulement assisté à des missions de sécurité des installations en entreprise.

Le Snaptain SP 500. Budget aux alentours de 150 euros. L'autonomie de la batterie est de 15 minutes mais le drone est fourni avec deux batteries. La distance de prise en main est de 220 mètres. C'est bien, mais ce n'est pas le matériel de la CIA. C'est plutôt un outil pour débutant car son inconvénient principal est qu'il sera détecté par les personnes au sol. A ce prix-là, ça reste un très chouette outil pour la détection de problèmes sur vos propres installations.

Le DJI Mavic Air 2 a une autonomie de plus de 30 minutes, prend des photos et des vidéos de très bonne qualité et une portée de 10 kilomètres. Il dispose d'une fonctionnalité de stabilisation dans les airs. Il vole à plus de 60 kms/heure mais je n'en vois pas bien l'intérêt pour le monde du renseignement. Son prix est de 849 euros.

4. La balise GPS pour filature à distance

La balise GPS appelée aussi tracker ou mouchard est un outil de suivi à distance. Vous savez que c'est interdit de l'utiliser à l'insu d'une personne, et c'est pour ça que tous les sites qui commercialisent ce genre d'outils les vendent avec des recommandations d'utilisation légale qui n'intéressent personne, mais l'honneur est sauf. De toute

façon, le fabricant dit que c'est pour assurer la sécurité de votre maman qui est Alzheimer en stade 3 ou pour veiller à ce que votre ado ne s'acoquine pas avec de sales petits voyous à casquette.

Dans notre monde, nous utilisons les balises pour suivre un véhicule en temps réel, sans se faire détecter. J'ai fait beaucoup de filatures dans ma carrière, c'est même l'une des raisons pour lesquelles j'ai choisi ce métier et j'ai très vite déchanté. Ça ne se passe pas du tout comme à la télé. Dans la réalité, vous perdez très souvent votre cible dans les embouteillages, vous vous prenez des amendes pour excès de vitesse que votre client refusera de payer et c'est d'un niveau de stress de fou. La balise GPS met un terme à tout ça avec un inconvénient somme toute mineur : c'est illégal d'en coller un sur le véhicule de votre cible. Idem pour le sac à main de madame, ce qui est aujourd'hui possible parce que le traceur fait la taille d'une carte de crédit, en plus épais quand même.

L'autre avantage du produit, c'est qu'une filature ne coute plus bien cher. Alors qu'avant, il fallait toute une équipée disponible h24, que le client trouvait scandaleusement chère. Maintenant, vous êtes confortablement installé, vous ne perdez jamais votre cible et vous n'avez pas le risque de vous prendre un 30 tonnes en pleine face parce que vous êtes obnubilé par les phares arrière de votre cible. On sait très bien que la plupart des gens achètent ce produit pour filer leur moitié.

Une autre utilisation de choix en milieu industriel et commercial est le suivi de marchandises si votre entreprise est victime de vols, ce qui arrive souvent. Avec une balise,

si votre chargement n'arrive pas à l'endroit prévu ou disparait de vos entrepôts, vous le saurez tout de suite et n'aurez plus qu'à appeler la police. Ici, l'utilisation du GPS est légale.

Il y a des modèles qui vont se glisser dans un sac ou dans une boite à gants, d'autres sont magnétiques, équipés d'aimants, et peuvent être posés sur un support métallique. Ces derniers peuvent notamment être fixés sous une voiture, les aimants sont suffisamment puissants pour résister aux secousses d'une route de campagne.

Le traceur GPS peut avoir plusieurs utilités. Il est sécuritaire pour protéger ou retrouver, et il peut évidemment être utilisé pour suivre quelqu'un à la trace. Son fonctionnement par GPS associé à une communication vers un smartphone, passe par une carte SIM ou un abonnement à un réseau privé.

Vous pouvez l'utiliser pour savoir si votre commercial passe bien ses journées chez les clients plutôt qu'au bistrot mais vous ne pourrez pas utiliser ces informations devant un tribunal.

Les critères pour choisir le GPS dont vous avez besoin sont :

- La taille
- L'autonomie. Choix cornélien car si vous voulez une autonomie de longue durée, il vous faudra une batterie plus grosse, qui rendra le traceur plus volumineux et donc moins discret. Tout dépend de

l'utilisation. Un traceur dans un container n'a pas besoin d'être spécialement discret.

- La facilité d'installation et de fixation. La fourniture d'un aimant est indispensable en cas de fixation sur un véhicule, si vous ne pouvez pas accéder à l'intérieur du véhicule.
- Fourni avec un boitier étanche
- Les frais de fonctionnement
- Choix de la carte SIM
- Choix de l'opérateur

Lors de l'achat d'un traceur GPS, les abonnements ou forfaits auprès d'un opérateur ne sont pas obligatoires. Rien n'interdit de supprimer le code PIN de la carte SIM et d'activer la fonction SMS pour que la balise GPS soit opérationnelle.

Mais avec un abonnement, vous pourrez suivre la cible en temps réel, alors que sinon, vous serez informé régulièrement par SMS de sa position. Si c'est pour une filature, la question ne se pose pas vraiment car vous avez à tout moment besoin de savoir où se trouve la cible. Alors que si c'est pour tracer des marchandises, ça me semble nettement moins indispensable. Enfin, rappelez-vous que la technologie a progressé de façon fulgurante ces 20 dernières années. Parler de traceur GPS n'a même plus de sens car la question à se poser est : de quel traceur ai-je besoin ?

Regardez ce petit gadget, le Cube. Il est minuscule, se cache dans une poche ou un sac. Son prix est de l'ordre de 20 euros, ce qui fait que le perdre n'est pas un drame. Il fait le boulot, mais si vous voulez tracer un container pendant 2 mois, je ne crois pas que ce sera l'outil idéal.

5. Regarder sous la porte. L'endoscope

La caméra endoscopique est traditionnellement utilisée en médecine et dans l'industrie. Sa mission consiste à voir là où il est difficile de voir à l'œil nu, que ce soit votre fondement ou la partie inaccessible d'une installation.
Nous l'avons tous vu fonctionner au cinéma ou dans des reportages par des équipes d'élite de la police afin de préparer une intervention quand il s'agit de voir ce qui se passe de l'autre côté de la porte, derrière une fenêtre ou en dessous du plafond. Donc, il est clair que cet outil peut être un précieux allié de l'agent de renseignement.

Les critères pour choisir un endoscope sont :

- Qu'il fonctionne sur batterie et pas sur secteur. Ce n'est pas l'idée du siècle de devoir chercher une prise en pleine nuit.
- L'autonomie de la batterie. Cela va de 30 minutes pour de l'entrée de gamme à plusieurs heures.
- La longueur du câble.
- La qualité du câble.
- Caméra étanche.
- Qualité de l'image. Full HD est un minimum.
- Fonction WI-FI avec application mobile.
- Réglage de la luminosité.
- Zoom.

- Pour le plus haut de gamme, ne nécessite pas l'utilisation de votre smartphone mais fonctionne avec un boitier autonome qui offre davantage de fonctionnalités.
- Fournit avec des outils complémentaires comme une perche si la caméra doit être placée en hauteur, une pince pour récupérer de petits objets ou un miroir pour voir à 90 degrés.

Les critères qui précèdent ne sont pas forcément des critères de qualité. Comme souvent avec le matériel, il s'agit d'acheter ce dont vous avez besoin. Si vous devez introduire le câble sous une fenêtre et que vous êtres en planque juste derrière, pas besoin d'une grande longueur de câble.

Le budget pour de l'entrée de gamme qui fonctionne correctement est de 25 à 30 euros. N'imaginez surtout pas que ces prix très bas sont l'indice d'un matériel de pauvre qualité. Vous en aurez pour votre argent. Le top de l'outil industriel vous coutera entre 150 et 250 euros.

6. Ecouter à travers la porte ou le mur. Le stéthoscope

Les microphones à contact mural sont des appareils professionnels, utilisés à des fins d'enquête, privées ou militaires. Ces dispositifs vous aideront à écouter les conversations à travers les murs de manière confidentielle et sûre, sans risque d'être détecté. Voyons ensemble à quoi servent les microphones muraux ou à contact et quels sont

leurs composants, afin de comprendre pleinement toutes les fonctionnalités de ces dispositifs d'écoute.

Un microphone mural est utilisé pour entendre à travers les murs, tout type de sons, grâce à des capteurs en contact direct avec les murs ou les plafonds jusqu'à 70 cm d'épaisseur. Un microphone de contact est composé d'une capsule microphonique, d'un diaphragme qui transforme les vibrations sonores en signaux audio, d'un processeur vocal et d'un préamplificateur. Un écouteur ou un enregistreur vocal numérique peut être connecté à la sortie audio. Ces outils sont capables de détecter tous les bruits, y compris les plus faibles, ce qui permet d'obtenir un son clair et stable. Ces appareils d'investigation ont un très bon rapport qualité-prix. On est évidemment très loin du stéthoscope de ce bon vieux docteur. Surtout, n'en achetez pas un pour vos missions de renseignement car il ne captera pas tous les sons.
Attention que les mots clés pour trouver ces produits NE SONT PAS « stéthoscope », mais plutôt « wall microphone », « microphone mural », « stéthoscope espion », « écoute murale » …

Les prix pour ce matériel vont de 10 à 150 euros. Certains produits ont un pouvoir de pénétration important, mais en général vous n'avez pas besoin de traverser plus de 25 centimètres. Vérifiez aussi qu'il est possible de raccorder votre appareil à un enregistreur, en tout cas si vous avez besoin de garder une trace de la conversation espionnée. Enfin, certains appareils vous permettent de trier les différents niveaux de sons. Dans la pratique, le matériel d'entrée de gamme est ici tout à fait bon.

7. Voir sans être vu : la mini caméra espion

Une bonne caméra espion peut avoir toutes sortes d'usages, même pour ceux d'entre vous qui ne sont pas des agents secrets. Les bonnes caméras espion se présentent sous différentes formes et tailles et peuvent être utilisées pour la sécurité domestique, ainsi que pour surveiller les enfants et les animaux domestiques lorsque vous n'êtes pas dans la pièce où ils se trouvent. Ou pour filmer illégalement vos employés en train d'essorer vos stocks pour s'assurer de plantureuses fins de mois. Encore une fois, tout renseignement obtenu illégalement vous sera parfaitement inutile devant un tribunal car vous ne pourrez pas présenter les preuves obtenues, même si elles sont incontestables sur le plan des faits.

Les caméras sont généralement peu coûteuses, et certaines sont même déguisées en objets ménagers comme des horloges ou des lunettes, ce qui vous permet d'être très discret. Certaines sont de simples petites caméras de la taille d'une pièce de deux euros, et parfois plus petites encore, qui peuvent être placées dans un endroit où la plupart des gens ne les remarqueront pas, tandis que d'autres sont déguisées en objets comme des cadres photo ou des clés USB. Comme vous pouvez l'imaginer, il existe de nombreuses possibilités créatives dans ce domaine.

Les caméras espion ont généralement un objectif grand angle, ce qui leur permet de capturer le plus d'espace possible dans une zone donnée. La qualité vidéo a tendance à varier. Certaines fournissent une vidéo de base et fonctionnelle, suffisante pour que vous puissiez voir ce qui

se passe, tandis que d'autres produisent des images de haute qualité.

Certaines caméras espion offrent également des fonctions supplémentaires utiles comme la vision nocturne ou la détection de mouvement, ce qui signifie qu'elles peuvent rester allumées plus longtemps sans avoir besoin de recharger leurs batteries.

Un autre avantage de la mini caméra, c'est sa facilité d'utilisation. Pas besoin d'être un expert pour l'installer. La technique et moi, nous ne nous sommes jamais vraiment rencontrés. Pourtant, il ne m'a pas fallu 15 minutes pour apprendre à installer ce genre de matériel.

Quels sont les critères d'achat ? Bien entendu, ces critères sont plus ou moins importants en fonction de l'usage que vous attendez de la caméra.

- L'autonomie. C'est le point faible de ce matériel. Une autonomie d'une heure est déjà un bon résultat pour un enregistrement live. Si la caméra enregistre

sur une carte mémoire, vous pouvez avoir une autonomie de deux à trois heures. Certaines caméras peuvent se brancher sur secteur mais pour la discrétion, ça complique les choses.

- Fournie avec différents supports. Par exemple avec une pince de fixation.
- La solidité du matériel et la résistance aux chocs.
- Qualité de la vidéo. Le full HD sera la définition minimum.
- Equipée d'un détecteur de mouvement qui économise la batterie puisque ne se déclenche que si quelque chose bouge dans l'environnement.
- Mode de vision nocturne.
- Enregistrement du son et qualité de l'audio.
- Dos magnétique afin de pouvoir la déposer rapidement sur tout support métallique.
- Vision en live ou enregistrement sur une carte mémoire. Pour voir en direct ce qu'il se passe, il faut un module WI-FI.
- Boitier étanche permettant un enregistrement en extérieur et même sous l'eau.
- L'angle de vue.

Les prix pour une caméra espion démarrent à moins de 15 euros. A ce prix-là, n'espérez pas jouer à James Bond. En

fonction de ce dont vous aurez besoin comme options, comptez entre 25 et 80 euros.

Quelques modèles plus exotiques de caméras espion

Les lunettes d'espionnage avec caméra intégrée.

Les lunettes espion sont parfaites pour les voyeurs qui veulent garder un souvenir de la plage et idéales pour une filature. D'une part, vous filmez en gardant les mains libres, et d'autre part, si vous voulez garder des images de votre filature, vous pouvez être en déplacement tout en filmant. Ça a l'air d'un gadget inutile et bien pas du tout. Il existe des modèles « ville » et des lunettes de soleil. C'est un bon outil quand vous devez filmer tout en étant en mouvement ou pour tout lieu où les caméras ne sont pas les bienvenues.

Avant tout achat, vérifiez que la caméra ne soit pas visible. Sur les modèles bas de gamme, on est à la limite du pitoyable et du ridicule. Ne vous attendez pas à produire un film de qualité. L'image est souvent un peu faible et la plupart des modèles sont très sensibles à la luminosité. Dès qu'il fait un peu sombre, on ne voit plus grand-chose. Les critères d'achat sont sensiblement les mêmes que pour une mini caméra espion. Sachez que certains modèles permettent la prise de photos et d'autres, pas. N'achetez rien en dessous de 50 euros si c'est pour un usage professionnel.

La caméra ampoule est une véritable ampoule, qui diffuse de la vraie lumière et qui s'installe dans une pièce où vous souhaitez filmer et enregistrer. Ça a l'air génial comme ça, pour filmer une réunion par exemple. Mais il vaut mieux que la lampe soit allumée quand les gens rentrent dans la salle de réunion, car la caméra est quand même visible. On compte sur le fait que nous n'aimons pas regarder une source lumineuse.

Il existe des tas de mini caméras espion. Faites votre marché en fonction de vos nécessités :

- Horloge murale
- Réveil matin (pour ceux qui en utilisent encore un)
- Clé USB
- Vis

- Bouteille (il s'agit d'une vraie bouteille en plastique)
- Prise de courant
- Montre
- Casquette
- J'en ai vu une planquée dans un déodorant et une autre dans une brosse à dents électrique.
- …

8. L’observation discrète en milieu urbain : le monoculaire

Le monoculaire, c’est comme des jumelles pour borgne. Lorsque vous faites de l’observation en ville, les jumelles manquent de discrétion. Certains monoculaires tiennent dans une main et c’est très pratique pour identifier une plaque minéralogique par exemple.
Il existe une grande variété de modèles et de tailles, en fonction de votre utilisation. Vous en avez avec vision nocturne, avec trépieds pour les longues observations à grande distance et même des répliques de longue-vue de pirate. Pour ce dernier modèle, je n’en ai jamais essayé et j’ignore si l’esthétisme à remplacé l’efficacité.
Les prix varient de 20 à plusieurs milliers d’euros. Si c’est juste pour observer discrètement en ville, l’entrée de gamme est ce qu’il vous faut.

9. Brouiller le signal d'un téléphone portable/d'un réseau WIFI ou d'un signal GPS

Un simple téléphone peut être utilisé pour espionner une réunion sensible. C'est même un excellent moyen de le faire car, contrairement au matériel présenté ici, si le téléphone est saisi, son propriétaire aura toujours le loisir de dire qu'il avait juste oublié son téléphone. Le meilleur matériel d'espionnage, c'est celui qui est utilisé par destination et pas par vocation initiale.

Un brouilleur vous garantit qu'aucun son ne sortira de la salle où vous vous trouvez. Il serait très utile aux enseignants qui perdent la raison à force de voir leurs élèves jouer avec leur téléphone durant tout le cours. L'utilisation de brouilleurs de téléphones cellulaires neutralise cette menace. Terminé, Facebook, pendant le cours sur l'histoire de la révolution française. Lorsqu'un brouilleur est activé, tous les téléphones mobiles présents dans la zone de couverture de brouillage sont bloqués. De grands humoristes d'entreprises l'ont aussi utilisé pour couper les communications de leur patron mal aimé. L'investissement est un peu élevé pour une bonne grosse blague, mais comme je l'ai vu faire, je le cite. Je reconnais que voir son boss secouer son téléphone pour le faire fonctionner est un des petits plaisirs de la vie. Ça peut être sympa aussi dans le train ou le métro quand votre voisin hurle dans son téléphone.

Enfin, plus embarrassant, sauf si vous êtes cambrioleur ou visiteur indésiré, beaucoup d'alarmes de maison sont des systèmes sans fil. La tentative de cambriolage par

brouillage empêche les réseaux de transmission de fonctionner. La communication entre votre système d'alarme et le centre de télésurveillance se fait via le réseau GSM. Si le réseau est bloqué, le lieu n'est tout simplement plus protégé.

Un brouilleur a donc une double vocation : vous protéger ou couvrir vos opérations.

Je n'ai pas trouvé d'enseigne belge, suisse ou française vendant ces produits, mais des sites dans un français approximatif avec des commentaires de toute évidence bidons. Ça ne veut pas dire qu'il s'agit d'arnaques mais probablement de sites miroirs qui se fournissent sur Alibaba. Tout ce que je vois vient de Chine. J'en ai reçu un en cadeau il y a quelques années et je n'ai pas demandé d'où il venait. Oui je sais que recevoir un cadeau de ce genre, c'est bizarre. Le monde du renseignement privé est bizarre.

Votre brouilleur prendra certainement plus d'un mois à arriver. Ce qui prend sens quand on sait que ces équipements sont interdits en France. Donc, ce sera Alibaba ou EBay. A partir de 100 euros pour un brouilleur efficace à quelques mètres. Plusieurs centaines d'euros pour du beau matériel qui interrompt la téléphonie portable, le réseau wifi et les signaux GPS. Il vous sera facile d'en acheter un, mais il y a toujours un faible risque qu'il soit saisi à la douane.

Avant tout achat, vérifiez que les fréquences utilisées dans votre pays correspondent aux fréquences compatibles avec le dispositif de brouillage.

10.Détecter les micros dans mon bureau

Le problème avec les détecteurs de micro, c'est que si votre appareil n'en trouve pas, vous ne savez pas si c'est parce qu'il n'y a aucun micro planqué ou si c'est parce que votre matériel ne vaut rien. Ou que vous ne savez pas l'utiliser. Je pense avoir utilisé ce matériel trois fois dans ma vie, et honnêtement j'avais un peu le sentiment de ne pas être à ma place. Un jour, j'étais chez un client important et il était convaincu que des micros étaient cachés dans son bureau car des informations confidentielles avaient fuité. Je lui dis que ça n'est pas ma spécialité mais comme on s'entend bien, il insiste pour que je m'en occupe. Je passe son bureau au détecteur et ne trouve rien. Puis le miracle survient lorsque nous sortons de son bureau. Au moment où il ferme la porte, un objet, je ne sais plus quoi, tombe par terre. Ça me donne une idée. Je demande à une dame qui passe dans le couloir de rentrer dans le bureau du boss et de compter à haute voix de un à dix. Je ferme la porte et nous entendons distinctement la dame compter. Je regarde le client. Il se marre. On a trouvé le « micro ».
Vous pouvez facilement acheter ce matériel, mais je vous le déconseille. Si vous craignez la pose de micros dans vos installations, faites appel à des professionnels.

11.L'amplificateur de sons

Un amplificateur de son a pour but d'écouter une conversation à distance, dans un espace public, et avec un maximum de discrétion. Raison pour laquelle, le modèle traditionnel d'amplification a, question discrétion, quelques soucis à se faire. Le modèle avec parabole est très bien,

mais comment voulez-vous utiliser ça à la terrasse d'un café ?

On en trouve aux rayons jouets ou dans le cadre de balades dans la nature. Si votre écoute se déroule en milieu ouvert et que la discrétion n'est pas un problème pour vous, ce matériel bon marché sera bien assez efficace.

Les meilleurs amplificateurs de son sont ceux créés à usage médical. Soyons clairs, on passe du budget d'un jouet à 20 euros à un système sophistiqué à 350 euros. Vous avez du bon matériel aux alentours des 100 euros.

L'appareil n'est pas invisible mais se remarque peu et surtout donne l'impression d'être un assistant auditif, ce qu'il est à la base. Les bons outils permettent de diriger la captation du son, et d'éliminer les bruits parasites. Certains ont une double application, écoute dans l'espace public et à travers une cloison, mais ça n'est pas le même usage. Si vous avez les moyens, offrez vous deux appareils distincts.

12.L'enregistreur de frappes clavier

L'enregistreur de frappes clavier, appelé aussi keylogger, est un petit logiciel qui s'installe très rapidement sur votre pc. Il enregistre dans un fichier dédié tous les échanges écrits sur la machine : textes en Word, conversations sur les réseaux sociaux, les codes secrets ainsi que les sites visités.
Ils sont presque toujours proposés pour veiller sur la sécurité de nos chers enfants mais c'est rarement leur réelle finalité. J'ai fait très peu de mission de surveillance de conjoint dans ma carrière d'enquêteur. Horreur de ça et puis ça se termine toujours mal car le pire est souvent vrai. Un jour, j'ai accepté une mission de ce genre. Le gars avait l'air tellement désemparé que j'ai dit oui. La filature de son épouse a duré moins de 30 secondes avant que je sois détecté. Soit je n'étais pas au sommet de ma forme, soit l'épouse était particulièrement méfiante. Comme il n'était plus envisageable de recommencer une filature, j'ai suggéré au client d'installer un keylogger sur l'ordinateur familial. Quand je l'ai revu, quelques jours plus tard, il m'a confirmé en pleurant que l'enregistreur de frappes clavier fonctionnait très bien. Son épouse n'avait pas un amant,

mais toute une collection d'amoureux. Ce fut la dernière fois que j'ai accepté ce genre de job.
Pour l'installer, il faut un accès physique à l'ordinateur. Certains keyloggers supposent d'avoir accès au pc pour récupérer les informations, d'autres les envoie vers une adresse de votre choix. Certains sont indétectables par un antivirus, d'autres demanderont que l'antivirus soit désactivé pour votre nouveau soft espion. Les données sont enregistrées dans un rapport caché, stockées sur le disque dur. Un raccourci clavier permet de rendre le programme invisible aux yeux des personnes qui utilisent le PC. Nous sommes ici clairement dans le cadre d'un usage familial et il n'est pas nécessaire d'utiliser du matériel haut de gamme.
« Revealer keylogger » est un outil gratuit qui fait très bien le travail. Il a cependant un inconvénient : si son activité n'est pas visible du bureau du pc, il reste actif dans le gestionnaire des tâches. Normalement, personne n'y va jamais à moins de s'y connaître ou d'avoir une bonne raison d'aller voir ce qui tourne sur la machine. Mais quand même, l'outil n'est pas totalement invisible. Tester le d'abord sur vous-même et faites-vous une opinion. S'il ne vous convient pas, vous en trouverez très facilement un autre.
https://revealer-keylogger.fr.softonic.com/

13.Le micro espion

L'option la plus simple pour enregistrer une conversation est bien entendu votre smartphone. Si vous pouvez le placer sur un bureau, tout est parfait. Mais si les choses se compliquent et que vous devez le planquer, le résultat n'y sera pas. A fortiori si vous le laissez dans votre poche

durant l'enregistrement car le son sera brouillé par le simple mouvement de vos vêtements.

Nous voyons dans ce chapitre qu'il existe des stylos espion avec une excellente capacité d'enregistrement. J'aime bien l'idée mais notre époque n'est plus trop aux Bics ni aux stylos.

Il existe toute une panoplie de micro espion pour toutes les occasions d'espionner son prochain. Cela sera exclusivement à vocation d'information car vous ne pourrez pas faire usage des informations obtenues devant un tribunal. L'utilisation du micro est très vaste. Le matériel est aujourd'hui d'excellente qualité et à des prix plus que démocratiques.

On peut dire qu'il existe deux types de micros espion : ceux que vous portez sur vous dans le cadre de l'enregistrement d'une conversation et ceux que vous cachez dans un endroit où vous ne serez pas durant l'enregistrement. Si vous êtes dans le deuxième cas, le meilleur matériel est celui qui dispose d'une carte SIM et qui fonctionne avec une couverture de réseau téléphonique. Vous appelez à partir de votre téléphone la carte SIM de votre espion et vous entendez tout ce qui se passe dans la pièce, tout en enregistrant la conversation. Certains modèles se déclenchent au moindre bruit. En général, l'appareil ne mesure que quelques centimètres et est assez facile à cacher. Il n'a qu'un inconvénient pour moi, c'est que si quelqu'un le trouve, il n'aura aucun doute sur ce dont il s'agit.

14. Le VPN

Un réseau privé virtuel (VPN) vous permet d'assurer votre vie privée et votre anonymat en ligne en créant un réseau privé à partir d'une connexion Internet publique. Il ne s'agit donc pas d'un matériel offensif comme la plupart de ceux que l'on trouve dans ce livre. Exceptionnellement, nous jouerons défense.

Les VPN masquent votre adresse IP, de sorte que vos actions en ligne sont pratiquement introuvables. Surfer sur le web ou effectuer des transactions sur un réseau Wi-Fi non sécurisé signifie que vous pourriez exposer vos informations privées et vos habitudes de navigation.

Autre avantage, si vous voulez accéder aux services d'un site étranger, vous verrez que parfois la connexion vous sera refusée parce que vous êtes dans un pays où le service n'est pas accessible. Avec un VPN bien configuré, vous pourrez faire croire à n'importe quel site que vous êtes dans n'importe quel pays. Par exemple, vivant en Thaïlande, sans VPN je ne peux pas accéder à certaines chaines de télé en ligne belges ou françaises. Ce qui n'est pas la fin du monde, mais imaginez-vous que vous vivez dans un pays ou Facebook ou Google sont interdits.

Si vous avez acheté ce livre, c'est peut-être par simple curiosité. Mais c'est aussi peut-être parce que vous avez l'intention de l'utiliser pour faire du boulot de renseignement. Dans le cas où vous restez soft, que vous surfez sur le net pour glaner gentiment de l'info, pas vraiment besoin d'un VPN. Mais si vous commencez à mener des opérations plus agressives et que vous ne voulez

pas vous faire repérer, un VPN est indispensable pour masquer votre IP véritable.

Si vous faites des choses louches, et encore tout dépend à quel point, il serait aussi bon d'avoir un ordinateur dédié à votre mission et pourquoi pas, utilisez le WI-FI du MacDo de la ville voisine. Cela étant dit, si vous faites quelques de vraiment pas bien, même le WI-FI du MacDo ne vous protégera pas car il y a des caméras de surveillance.

Quelques critères pour choisir votre VPN :

- La simplicité. Un VPN en français sera souvent plus facile à utiliser. Mais en général, utiliser un VPN ne vous demande pas d'être ingénieur. Si je peux, tout le monde peut. Il s'agit juste de télécharger un soft et de le configurer un peu. Comme je ne suis pas ici pour discuter de votre connexion à Netflix US ou à un site de téléchargement illégal, mais dans le cadre de vos prochaines missions de renseignement, en gros, tout ce dont vous avez besoin, c'est de ne pas être traçable et qu'on vous croit dans un pays où vous n'êtes pas. Même si vous avez le QI d'une asperge, vous devriez faire ça en trois clics.

- Que voulez-vous faire avec votre VPN ? Vous visez un pays en particulier, besoin d'accéder à de nombreux pays ? Certains VPN ne donnent pas accès à tous les pays.

- La compatibilité avec votre machine.

Il existe beaucoup de VPN gratuits, mais je ne vous les conseille pas. Ils sont en général moins sécurisés et moins

performants. Pratiquement tous les VPN se valent et les abonnements payants sont très bons marchés, à partir de 2 euros par mois. Pour ma part, j'utilise Cyberghost depuis longtemps. C'est l'un des leaders mondiaux si ça peut rassurer.

https://www.cyberghostvpn.com/fr_FR/

15. Clonage de disque dur ou de téléphone

Le « forensic cloning » ou clonage médico-légal, également connu sous le nom d'image médico-légale ou d'image à flux binaire, est une copie exacte, bit pour bit, d'un élément de preuve numérique. Il capture tout, du début à la fin. Grâce à cette méthode, les fichiers, dossiers, disques durs, etc. peuvent être clonés et conservés totalement à l'identique.

Le clonage médico-légal de téléphones portables consiste à produire une copie exacte de l'ensemble d'un téléphone portable. Il est réalisé sur les appareils mobiles qui pourraient servir de preuve devant un tribunal.

Un clonage n'est pas pareil à un copié/collé. On pourrait croire que si, ben non. Le clonage médico-légal est une copie exacte d'une preuve numérique, y compris toutes les données supprimées ou détruites, tandis que le copié/collé ne concerne que les fichiers et dossiers présents sur l'appareil.

Les données trouvées grâce au clonage médico-légal peuvent être utilisées comme preuves devant un tribunal. Sauf si vous avez obtenu les informations de façon illégale.

Il existe une foule de logiciels permettant le scan d'un pc ou d'un téléphone. Si vous devez avoir un scan parfait d'un appareil, si vous devez récupérer des données effacées ou si l'appareil est partiellement détruit. Si vous n'êtes pas un spécialiste de l'investigation informatique, n'y pensez même pas. Ou plutôt si, mais faites appel à un pro.

16. Outils de cryptographie

La cryptographie est associée au processus de conversion d'un texte ordinaire en texte inintelligible et vice-versa. C'est une méthode de stockage et de transmission de données sous une forme particulière afin que seuls ceux à qui elles sont destinées puissent les lire et les traiter.

Un exemple de cryptographie de base est un message crypté dans lequel les lettres sont remplacées par d'autres caractères. Pour décoder le contenu crypté, il faut une grille ou un tableau qui définit la manière dont les lettres sont transposées. Cette méthode est utilisée depuis des siècles.

Aujourd'hui, il existe des outils de cryptographie et ces outils utilisent bien entendu l'informatique. Vous les utilisez pour que vos mails envoyés ne soient compris que par la bonne personne. Pour qu'il soit impossible de lire les documents que vous rédigez. Pour empêcher l'accès à vos données si vous avez fait de grosses bêtises et que les gentils policiers saisissent votre matériel informatique avant de vous envoyer vous détendre un peu en cellule.

L'époque de l'envoi de messages cryptés où on utilisait uniquement le déplacement des lettres de l'alphabet est un

peu dépassé. Ecrire un message où le P devient W en est un exemple. Le code est fort simple à casser.

Axcrypt fera formidablement bien le boulot, sans bourse délier, si vous êtes sous Windows. Si vous avez un Mac, on suppose que vous avez les moyens et il vous faudra payer. Une version IOS ou Android existe pour votre téléphone.

https://www.axcrypt.net/

17. Un téléphone jetable anonyme

Depuis quelques années, il n'est théoriquement plus possible d'acheter un téléphone jetable avec carte SIM intégrée, de façon anonyme. Dans sa légitime lutte contre les malfrats et terroristes de tout poil, de nombreux gouvernements ont exigé que l'achat d'une carte SIM soit lié à une identification. Ce qui est très modérément pratique pour quelqu'un œuvrant dans le renseignement.

Un téléphone anonyme a deux fonctions essentielles : émettre ou recevoir des appels anonymes et être le moins détectable possible.

Dans un monde parfait, le téléphone jetable est prêt à l'emploi : batterie chargée, carte SIM intégrée, avec du crédit. Vous pouvez trouver ça dans n'importe quelle boutique, mais ce ne sera pas anonyme.

Il vous faudra acheter les deux séparément.

Votre téléphone aura comme caractéristiques indispensables :

- Pas de smartphone. Un smartphone vous aide à vous tracer avec les applications en ligne que vous utilisez. Donc, un téléphone à l'ancienne sans internet. Nokia faisait les meilleurs, les plus solides, et avec une autonomie allant jusqu'à une semaine.
- Qu'il ne sera JAMAIS utilisé pour appeler un proche.
- Qu'il ne sera JAMAIS ouvert dans un endroit que vous fréquentez régulièrement.
- Qu'il ne sera JAMAIS allumé à côté de son grand frère, votre smartphone.
- Qu'il sera éteint quand vous ne l'utilisez pas et emballé dans une « silent pocket » qui empêche l'émission ou la réception d'ondes. Vous en trouverez sur Amazon sans problème. Pas besoin d'être anonyme pour en acheter une.

Mais il vous faut encore carte SIM et recharge. Que vous trouverez sans problème dans des pays comme la Thaïlande ou l'Ukraine. Pas besoin d'y aller, vous pouvez vous faire envoyer tout ça par la poste. Pensez à acheter de lourdes recharges car les communications vont vous coûter un os. Sinon, un site vous permet d'acheter des cartes SIM anonymes : https://simslife.fr/

Le site n'a pas l'air d'être situé sur le sol français. Je n'arrive pas à le localiser. Je ne leur en veux pas de ne pas vouloir être traçable. Si vous utilisez cette carte SIM avec un smartphone, pensez bien que c'est exactement comme si vous téléphoniez depuis l'étranger. Désactivez certaines

fonctions sur votre téléphone, sinon votre crédit sera dévoré en dix minutes.

18. Un lecteur de carte SIM pour lire les SMS d'un téléphone éteint

Si vous voulez lire les SMS envoyés par votre cible, c'est possible sans devoir installer un logiciel espion. Il faut pour cela récupérer la carte SIM du téléphone cible, l'insérer dans le lecteur de cartes et connecter le lecteur à votre pc. Vous aurez accès aux SMS de la carte, y compris ceux qui ont été effacés. Le lecteur de carte SIM ne vous permettra pas d'avoir accès aux applications de messagerie ni aux réseaux sociaux du téléphone cible, mais reste une bonne source d'informations quand vous pouvez accéder au téléphone cible quelques minutes, mais que vous n'en connaissez pas le code d'accès.

19. L'écoute d'un portable à distance. L'IMSI Catcher

Vous avez vu ces agents dans un film qui se connectent en deux clics au réseau GSM de leur cible pour écouter tranquillement la conversation. Si vous aviez un jouet comme ça, vous en feriez quoi ?

Un IMSI Catcher est une technologie intrusive qui peut être utilisée pour localiser et suivre tous les téléphones portables qui sont allumés dans une certaine zone. Actuellement, jusqu'à un kilomètre. L'IMSI Catcher fait cela en "se faisant

passer" pour une tour de téléphonie mobile, en trompant votre téléphone pour qu'il s'y connecte et en révélant ensuite vos données personnelles à votre insu.

Les IMSI Catchers sont des outils de surveillance qui peuvent être utilisés pour suivre les personnes qui assistent à une manifestation, à un événement public, pour surveiller vos appels et modifier vos messages ou pour localiser une cible avec précision. Normalement, ces outils sont exclusivement réservés aux services d'état, mais j'espère que tout le monde a compris que ce concept est totalement dépassé. J'ai fait des demandes de renseignements auprès de divers fournisseurs. Soit je n'ai reçu aucune réponse, soit on m'a signalé que ça n'était pas pour moi. Aucun fournisseur européen ou américain ne m'a fait parvenir renseignements ou offres.

Mais sur Alibaba, à partir de 1500 dollars pour le modèle d'entrée de gamme, l'éthique s'achète. On peut penser que d'ici un an ou deux, on pourra enlever un zéro à ce prix.

20. La carte de crédit anonyme

Dans le cadre de missions de renseignement, vous serez sans doute amené à devoir faire des achats en ligne ou à prendre des abonnements sur certains sites. Dans ce cas, vous ne voulez pas être tracé. Les gouvernements luttent depuis longtemps contre ces systèmes de paiements car ce sont des outils traditionnels du terrorisme et du blanchiment d'argent. Vous pouvez très facilement trouver une carte prépayée, mais depuis janvier 2020, l'anonymat n'est

garanti que jusqu'à un plafond de 150 euros. Si c'est assez pour vous, pas de problème, vous en trouverez partout.

Si votre mission vous demande des ressources plus importantes, les solutions existent. Vous pouvez créer un compte dans un endroit comme : Anguilla, les Bahamas, les Fidji, l'île de Guam, les îles Vierges américaines, les îles Vierge britanniques, le sultanat d'Oman, le Panama, les Samoa américaines, les Samoa, les Seychelles, Trinité-et-Tobago et le Vanuatu. Le secret bancaire y est absolu. Attention, cette liste change régulièrement. Une fois que vous avez un compte, vous obtiendrez très facilement une carte de crédit totalement intraçable. Des établissements suisses vous promettront la même chose, mais il y aura toujours un risque.

Chez Vadiance par exemple, vous pouvez obtenir une carte de crédit anonyme avec des fonds provenant de n'importe quelle banque. Il vous sera simplement demandé un IBAN.

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

Dans la première édition de ce livre, je vous proposais une liste de lieux où vous pouviez acheter tous ces outils de travail. Aujourd'hui, pratiquement tout se trouve sur Amazon. Y compris le haut de gamme. Pour chaque produit, vous avez les commentaires des clients et c'est un avantage précieux. Ces évaluations constantes ont aussi mis les fournisseurs sous pression. Un appareil de mauvaise qualité, un service bas de gamme, et c'est terminé. Il y a dix ou quinze ans, si un client n'était pas content, ça n'avait pas beaucoup d'impact. Avec du matériel technique, un avis

négatif ne signifie rien. Il est possible que le client se soit énervé sans avoir lu le mode d'emploi.

Cependant sur Amazon, pas d'explication. Si vous avez besoin d'assistance, il vaut mieux faire vos emplettes sur un site spécialisé où on vous répondra en français.

https://www.hd-protech.com/ avec un magasin à Marseille

https://www.macameraespion.com/

https://www.yonis-shop.com/

https://www.boutique-espion.fr/

https://securvision.fr/ avec un magasin à Paris

VI. Débusquer les mensonges d'un CV

Beaucoup de recruteurs, professionnels ou non, se fient à leur instinct lors d'une procédure de sélection. L'intuition n'est rien d'autre qu'une projection de soi-même. Ceux qui pensent qu'ils ont du flair sont ceux qui se trompent le plus.

Deux catégories professionnelles ont un taux élevé de faux CV : les cadres dirigeants et les commerciaux. Il est vrai que si vous êtes maçon, il est particulièrement stupide de mentir puisque votre incompétence sera découverte en une demi-heure. Plus une fonction est élevée dans la hiérarchie de l'entreprise, plus vous aurez de temps pour faire vos preuves. Ce qui dans certains cas, vous permettra d'acquérir les compétences que vous n'aviez pas au départ.

Je ne porte pas de jugement sur ces mensonges. Certains de mes clients ont décidé d'engager un candidat tout en sachant qu'il avait menti dans son CV. Ceux-là l'ont fait en connaissance de cause. Un jour, j'ai eu un candidat qui, avant de démarrer l'entretien, me dit ceci :

« Autant ne pas perdre de temps. Dans mon dernier emploi, j'ai été viré pour faute grave et la faute grave était justifiée. Je m'assieds ou je m'en vais tout de suite ? »

Comme à peu près tout le monde à ma place j'imagine, je lui ai proposé de s'asseoir. Pour résumer, sa femme l'avait quitté et un soir qu'il rentrait du boulot, il a constaté qu'en partant, elle avait absolument tout emporté, jusqu'au porte-manteaux. Il a commencé à boire. Puis à faire de faux rapports de visites et a provoqué un accident avec la voiture

de la société en étant ivre. J'ai raconté cette anecdote à des tas de gens. Tout le monde a réagi de la même manière, « oui, c'est pas bien, c'est normal de se faire virer mais bon,… ». Le gars n'était pas honnête, il était malin. Il savait que je le découvrirais de toute façon. La sensation n'est pas la même si le candidat aborde le sujet ou si je le découvre. Il a misé sur ça et il a gagné. Le client a juste dit « s'il est capable de vendre une faute grave, il va casser la baraque chez nous ». Ce qu'il a fait.

Je comprends certains candidats. Entre mentir et rester au chômage ou dans un job sans perspective, le choix est vite fait. Vous n'avez pas forcément envie d'avouer que vous avez complètement raté vos études, que vous avez passé deux ans en prison ou que vous êtes resté cloué dans votre lit pour dépression. Les choses ont totalement changé aujourd'hui, mais au début de ma carrière, les candidats qui avaient choisi de voyager autour du monde pendant un an ou deux, étaient très mal perçus. Bien sûr qu'ils s'inventaient des jobs à l'étranger.

Si je peux faire preuve d'empathie, cela ne signifie pas que je vais accepter. Si mon boulot est de traquer le baratin, je traque.

Votre entreprise va dépenser des milliers d'Euros lors d'une procédure de recrutement et sélection : publicité, cabinet de recrutement, heures passées, tests et assessment, formation du nouveau collaborateur…

La procédure qui vous est proposée ici prendra entre 2 et 5 heures. Elle devrait faire partie intégrante du processus pour tous les candidats en phase finale de sélection.

Clairement, ce n'est pas ce qui se pratique aujourd'hui en Belgique ou en France.

La vérification des éléments factuels du CV commence doucement à rentrer dans nos mœurs. Pour certaines entreprises ou cabinets de recrutement, ce qui suit fait partie de la procédure habituelle. Tous ceux qui ont passé du temps à vérifier ces éléments sont tombés sur des histoires extravagantes.

1. Demander l'accord du candidat

Il est dans l'intérêt du recruteur de demander l'accord du candidat avant de se lancer dans un processus de vérification de références.

D'abord, pour des raisons légales. Si vous travaillez dans un cabinet de recrutement, la plupart des associations professionnelles du secteur imposent à leurs membres d'obtenir l'accord du candidat avant de se lancer à la chasse aux infos. Mais si vous êtes un professionnel du renseignement ou la personne responsable du recrutement dans votre société, vous avez largement intérêt à avoir cet accord car si vous nuisez à la carrière du candidat en vérifiant ses références, celui-ci peut se retourner contre vous.

L'autre raison est davantage pratique. A la fin d'un entretien, posez une question comme « D'après vous, que me dirait votre ancien patron si je lui demandais comment s'est passé votre collaboration ? »

Vous observerez sur le visage du candidat une expression fugitive, qui peut être :

- La peur/l'inquiétude
- La colère
- La totale assurance
- L'embarras
- La déception
- La surprise
- La nervosité
- Le contentement

La plupart des candidats répondent qu'il n'y aura pas de problème et que leur ancien patron donnera d'excellentes références. C'est la réponse socialement acceptable et le candidat sait très bien que toute autre réponse nuira à la poursuite du processus de sélection.

Certains cependant vous expliqueront d'un air embarrassé que tout ne s'est pas passé pour le mieux et qu'il est préférable de ne pas le contacter. Vous apprendrez alors que le départ du candidat ne s'est pas déroulé dans les conditions idylliques qu'il vous a expliquées durant l'entretien. Vous venez de gagner un temps précieux.

2. Quelles références demander ?

La seule référence pertinente est celle de l'ancien supérieur hiérarchique. Le DRH n'est pas totalement inutile, mais vous n'obtiendrez ici que quelques éléments factuels : confirmation que le candidat a bien travaillé pour la société, intitulé de fonction, date d'entrée et date de sortie.

Les anciens collègues, clients ou fournisseurs sont de peu d'intérêt car ils auront été choisis avec soin par le candidat.

Pour votre propre sécurité, vous demanderez au candidat de signer un document vous autorisant à vérifier les références. Ce document comprendra une liste nominative des anciens supérieurs hiérarchiques que le candidat vous autorise à contacter. Si vous êtes un prestataire de services engagé pour la vérification du CV, vous aurez pris soin de vérifier que votre client a bien obtenu cet accord écrit.

3. A quoi être attentif lors de la demande de références ?

Ce qui suit est une liste non-exhaustive de situations où votre radar de recruteur devrait commencer à clignoter.

Le candidat affirme qu'il travaillait pour une entreprise dirigée par un membre de sa famille.

Le candidat ne se souvient pas du nom de son précédent manager.

Le candidat vous donne le numéro de portable de son ancien patron. Ce peut être pour vous faciliter la tâche ou

parce qu'un ami décrochera à ce numéro en se faisant passer pour la référence.

La précédente entreprise du candidat a fait faillite ou a été rachetée. La vérification sera encore plus complexe si cette entreprise est située à l'étranger.

Le précédent dirigeant a quitté la société et le candidat ne sait pas où il travaille aujourd'hui.

La référence donnée par le candidat ne parle ni français ni anglais ni néerlandais.

La référence vit dans un pays qui vous obligera à téléphoner au milieu de la nuit.

Le dirigeant est pensionné ou décédé.

Ce qui précède ne signifie en aucune façon que le candidat veut vous cacher quelque chose. C'est seulement possible. Si une des situations précédentes se produit, vous savez que votre totale vigilance est indispensable. Je suis toujours parti du principe que ce que dit le candidat est vrai jusqu'à preuve du contraire. C'est la différence entre la suspicion paranoïaque et la prudence bienveillante.

4. Vérifier le diplôme

Beaucoup d'entreprises ne vérifient pas correctement que le candidat possède bien le diplôme qu'il prétend avoir. Il arrive souvent qu'on demande une copie du diplôme ou même l'original. C'est une méthode largement insuffisante

aujourd'hui tant il est facile de fabriquer ou d'acheter un faux.

C'est pourtant ici que beaucoup de candidats mentent. Principalement les hauts profils. Plusieurs études convergent vers les mêmes chiffres : 20 % des candidats à un poste de haut niveau mentent sur leurs diplômes.

Les principaux mensonges sont :

- « Formation » ne donnant lieu à aucun diplôme
- Fréquentation de l'école mais sans obtention du diplôme
- Exagération du niveau réellement obtenu
- Difficulté à évaluer le niveau du diplôme par l'utilisation de sigles compliqués
- Invention pure et simple d'une université fantôme
- Contrefaçon d'un diplôme
- Faux acheté sur internet

Pour vous convaincre de la facilité avec laquelle on peut acheter un diplôme en ligne, je vous suggère de lancer la recherche « buy fake diploma » sur Google. Maintenant, vous savez qu'en cas de besoin, vous pouvez être neurochirurgien la semaine prochaine.

Il n'existe que deux moyens fiables de vérifier cette information. Soit en contactant directement l'école (par mail ou par téléphone) soit en regardant si le nom du candidat est présent dans le répertoire des anciens diplômés. Je suis déjà tombé sur une organisation qui avait créé

plusieurs sites internet d'universités bidons, avec faux nom, faux blason…

Quand il s'agit de formations à l'étranger, il est parfois difficile de comprendre le niveau réel du diplôme. Par exemple, une formation d'été en management à Harvard peut vite se transformer en MBA. Les MBA ont particulièrement la cote sur le grand marché du mensonge et la prestigieuse université d'Harvard semble avoir l'affection des fraudeurs. Grave erreur, car l'université d'Harvard répond dans l'heure à toute question relative à ses anciens diplômés.

5. Vérifier les antécédents

Il n'est évidemment pas question ici de vérifier l'éventuel casier judiciaire d'un candidat. C'est tout à fait illégal et stupidement risqué. En plus, il suffit de demander un certificat de bonne vie et mœurs, pour les belges en tout cas. Le premier outil de vérification est Google. Vous tapez le prénom et le nom du candidat entre » ».

Vous aurez la possibilité de trouver photos, vidéos, documents, brevets déposés, articles de journaux où le nom du candidat est cité… Il existe beaucoup de techniques permettant d'affiner vos recherches via Google, mais j'imagine que pour une vérification de candidature, il n'est pas indispensable de mener une véritable enquête approfondie.

Vous irez aussi faire un petit saut rapide sur le profil Facebook du candidat. Le but de cette démarche n'est pas

d'obtenir des informations sur la vie privée du candidat. Si vous trouvez une photo de votre futur marketing manager en train de danser torse nu sur une table, ça ne vous apprend pas grand-chose d'utile. Cependant, si vous apprenez via une photo de presse qu'il a été placé en garde à vue, ça mérite un approfondissement. Tout comme si vous trouvez un message sur son mur Facebook, le félicitant pour son nouveau job chez votre principal concurrent. Ou ses interventions dans des forums ou blogs en faveur de la suprématie blanche. Vous risquez aussi de trouver n'importe quel élément factuel qui contredit un élément important de son CV.

Est-ce qu'il est fréquent qu'on découvre ce genre de choses ? Non. Mais suffisamment pour que la vérification soit systématique.

Vous prendrez soin aussi de vérifier auprès du registre du commerce que le candidat n'est pas à la tête d'une entreprise qu'il aurait oublié de mentionner. Même si c'est le cas, ce n'est pas forcément rédhibitoire, mais il est quand même important que vous en soyez informé.

6. Contacter une référence

Le contact avec une référence donnée par le candidat se fait par téléphone. Il est très rare qu'une personne refuse de parler à un recruteur au téléphone, quand il s'agit d'une vérification de références. J'ai souvent vu des recruteurs faire de la vérification de références par mail. Autant ne rien faire. Souvent, on ne vous répondra même pas.

Si vous attaquez directement avec une question aussi vague que « je voudrais savoir comment s'est passé la collaboration avec Mr X. ? », vous risquez d'embarrasser le répondant et d'obtenir une réponse aussi riche que « ça s'est bien passé ».

Pour commencer en douceur, vous vérifiez les informations purement factuelles :

- Intitulé de la fonction
- Date d'entrée
- Date de sortie
- Contenu de la fonction
- Raison de départ

Rien qu'avec ça, vous ne manquerez pas de surprises.

S'il s'est passé quelque chose de grave, le répondant n'attendra pas qu'une question lui soit posée avant de déballer son sac. Mais même quand la collaboration s'est mal passée ou mal terminée, beaucoup de répondants répugnent à en parler spontanément.

Par exemple, si le candidat postule une fonction où il aura à gérer une équipe, il vaut mieux ne pas demander « comment était Mr X. en tant que manager d'équipe ? » mais plutôt « que devrait améliorer Mr X. pour être un meilleur manager ? » Ou « dans quel genre de fonction voyez-vous idéalement Mr X. et pourquoi ? »

Je suppose que je ne vous apprends rien en vous faisant remarquer qu'ici, nous sommes dans le registre de l'opinion

et pas du fait. Il est certainement intéressant d'avoir l'opinion de l'ex-manager, mais ça reste fort subjectif. Vous ne savez pas et vous ne saurez jamais ce qu'il s'est passé entre ces deux personnes. Quand vous avez la chance de pouvoir vérifier plusieurs références et que les commentaires vont dans le même sens, vous pouvez penser que vous approchez de la vérité.

Un jour que je vérifiais la référence d'un commercial, son ancien manager m'a simplement répondu « dites lui qu'il peut revenir quand il veut ». Je pense qu'il a eu le poste.

7. Cas de figure

a) Le candidat affirme qu'il travaillait pour une entreprise dirigée par un membre de sa famille.

- Demander au candidat de présenter des fiches de rémunération

- Poser au dirigeant de la société les questions du point 6. Un membre de votre famille sera certainement disposé à prétendre que vous avez travaillé dans sa société, ce qui ne veut pas dire qu'il aura prévu un mensonge élaboré.

Soyons humbles, dans ce cas de figure il n'y a pas grand-chose à faire. Demander à un ami ou à un membre de la famille de servir de référence est pratiquement indétectable, à moins de mener une enquête approfondie. J'avoue l'avoir déjà fait pour un ami.

b) La précédente entreprise du candidat a fait faillite ou a été rachetée.

- Vérifier que c'est vrai aux dates mentionnées par le candidat
- Demander le nom de l'ancien responsable direct et idem que le point 6.

c) Le précédent dirigeant a quitté la société et le candidat ne sait pas où il travaille aujourd'hui.

- Vérifier que l'information est fondée
- Nous sommes à une époque où la plupart des cadres et dirigeants laissent une trace sur le web. Vous devriez pouvoir le retrouver assez facilement via les réseaux sociaux

d) Le candidat est toujours en fonction et travaille depuis plusieurs années chez le même employeur

Bien entendu, vous ne pouvez pas vérifier les références du candidat sans lui nuire gravement. Cependant, ce qui est très facile à faire, c'est de vérifier si c'est vrai. En effet, beaucoup de candidats ayant perdu leur emploi choisissent de mentir à ce sujet. C'est bien compréhensible puisqu'un candidat en fonction a plus de valeur aux yeux d'un employeur.

Le plus simple ici, c'est de contacter l'entreprise en question par téléphone et de demander à parler au candidat. Si vous entendez en réponse « je vous le passe », vous raccrochez.

Pour info, il m'est déjà arrivé plusieurs fois d'apprendre de cette façon que non seulement le candidat n'y travaillait pas mais n'y avait jamais travaillé. Une fois cette étape réalisée, vous avez la confirmation que le candidat est toujours en activité, ou pas. Si l'information est confirmée, vous devez au moins savoir s'il exerce bien la fonction mentionnée dans son cv.

Souvent, vous trouverez cette information sur le site de la société. Sinon, si le candidat a affirmé qu'il exerçait une fonction de responsable de la production, vous téléphonez à l'entreprise en disant que vous devez envoyer un mail au directeur de la production, « s'agit-il bien de Mr X. ? ». Si la technique est un peu tordue, elle a quand même l'avantage de vous donner une information très importante sans nuire au candidat. Et honnêtement, il est courant que des candidats s'inventent des fonctions et des responsabilités. C'est le mensonge le plus courant.

Dernier point, et non le moindre : la procédure de vérification idéale doit comprendre les derniers candidats en lice pour le poste. Ou vous le faites de façon systématique, ou vous êtes certain que vous vous ferez avoir. Les sociétés où une vérification est effectuée « quand il y a un doute » sont celles qui ne détecteront pas les bons menteurs.

VII. TOUT SAVOIR SUR VOS CONCURRENTS

« Les affaires, c'est la guerre. Et la guerre, ce sont les affaires ». Cette citation n'est ni l'œuvre d'un grand guerrier, ni d'un génie des affaires, mais de Kevin Anderson, un auteur de science-fiction. Je n'ai pas d'opinion sur la deuxième partie de sa phrase, mais suis plutôt en accord avec le début de la citation. Le commerce suppose une compétition entre concurrents. Le plus fort, le plus rapide, le plus intelligent, le mieux adapté, gagne. Contrairement à la vraie guerre, le ou les perdants ne meurent pas. Ils perdent des parts de marché et puis parfois rebondissent, parfois disparaissent. La clé des guerres modernes est le renseignement. Terminé d'envoyer 10.000 gars baïonnette au canon, à l'assaut d'une position ennemie, sans savoir ce qui attend les soldats à l'arrivée. La plupart du temps, le pire.

Jusqu'au XXème siècle, les espions étaient méprisés avant de devenir à notre époque, les héros des conflits modernes. Le chef d'entreprise qui ne se préoccupe pas de ses concurrents est comme ces généraux du passé qui envoyaient leurs troupes se faire massacrer au nom de l'honneur. La différence avec la guerre, et je m'en réjouis, c'est que quand votre entreprise aura disparu par manque d'anticipation, vous ne mourrez pas. Pas physiquement en tout cas.

Dans les chapitres précédents, nous avons déjà vu divers outils utiles à l'analyse concurrentielle, inutile de recommencer. Une courte synthèse suffira :

- La recherche booléenne et le Google Hacking
- GOOGLE IMAGES et la localisation de photos
- Google vidéo
- Google Alert

Nous allons voir dans ce chapitre, que le renseignement privé se divise en plusieurs branches. En ce qui nous concerne, notre travail appréhendera principalement deux sphères du renseignement, le HUMINT et LE OSINT, le renseignement d'origine humaine et le renseignement à partir de sources ouvertes.

1. Le renseignement humain pour tout savoir de ses concurrents et (futurs) partenaires

Selon la définition de la CIA, humint (human intelligence) est tout simplement toute information obtenue de source humaine. Les méthodes utilisées ne s'opposent pas aux autres sources de renseignements. Elles en sont soit un complément, soit la dernière source utilisée quand toutes les autres ne fonctionnent pas. Le renseignement humain est ce qui se fait de plus complexe et de plus coûteux. Ces opérations peuvent être légales ou illégales, certaines demandent la création d'un scénario. Le renseignement humain comprend aussi les domaines de l'ingénierie

sociale, à savoir les techniques qui permettent d'obtenir des informations de la part de votre cible sans qu'elle s'en rende compte.

L'ingénierie sociale, c'est avant tout de la manipulation. Lorsque vous entendez à la télé qu'un cadre a viré une grosse somme d'argent de son entreprise parce qu'il s'est fait avoir au téléphone par un escroc, vous vous dites « mais quel con, c'est pas possible d'être aussi con ! ».

Vous êtes absolument certain qu'avec vous, ça ne marcherait jamais. Psychologue de formation, j'ai enseigné la manipulation et les comportements d'influence dans de grandes entreprises belges et françaises. Je sais, ce n'est pas beau, mais qu'est-ce que c'est drôle. 100 % des participants étaient convaincus que les autres étaient manipulables, mais pas eux. Ce qui fait que les techniques de manipulation fonctionnent, c'est la croyance chez les humains, qu'elles sont inefficaces sur eux. Cette croyance en notre force est notre première fragilité.

Vous devez avoir une force de persuasion et une assurance en vous en dehors du commun pour convaincre un humain de faire ce que vous voulez. Quand vous marchez dans la rue, les gens sont surpris que le trottoir ne vous colle pas aux semelles tellement il est évident que la rue vous appartient. Vous n'êtes jamais ni surpris ni décontenancé. Nous verrons plus loin que l'empathie, l'écoute et la synchronisation sont des compétences essentielles de l'agent de terrain.

Nous allons voir ici une série de techniques permettant d'obtenir des informations de sources humaines. Certaines sont très simples à mettre en place, d'autres demandent une

mise en place complexe. Tout dépend de l'énergie que vous, ou votre organisation, êtes prêt à dépenser pour obtenir ce que vous voulez.

Il est également important d'enregistrer le plus grand nombre possible de ces informations au moment de leur collecte. Non seulement pour documenter les preuves, mais aussi pour éliminer les préjugés personnels. À titre d'exercice, assistez parfois à une réunion d'une heure, enregistrez-la et, quelques jours plus tard, essayez de noter les éléments essentiels de ce que vous avez entendu. Ensuite, repassez l'enregistrement et notez vous-même vos souvenirs.

Pour chacune de ces activités, un briefing avant l'événement et un débriefing après sont toujours une partie importante du processus car certains membres de l'équipe peuvent avoir relevé une pépite que d'autres ont manqué.

L'écoute passive

La technique la moins efficace et la plus facile à utiliser de notre liste est l'écoute passive. L'auditeur passif HUMINT est une éponge, qui absorbe toutes les informations de n'importe quelle voix dans la pièce.

L'écoute passive se pratique dans les lieux publics ou accessibles au public où des gens susceptibles de vous fournir de l'information se rendent. Bar, restaurant, salon professionnel, aéroport, cafétaria d'entreprise si elle est facile d'accès…

Contrairement aux autres techniques du renseignement humain, celle-ci ne vous demande pas de grandes compétences, si ce n'est la patience. Le vendredi soir après le boulot, les employés de l'entreprise que vous espionnez se rendent dans un bar pour boire quelques verres. Logiquement, on devrait se dire qu'à notre époque, où l'on parle de sureté avec autant de régularité, les cadres se font discrets. Pas du tout. Le drink du vendredi soir est l'occasion de vider son sac avec tout ce qui ne fonctionne pas au boulot. Ça tombe bien, c'est justement ça qui vous intéresse !

Il y a peu de temps, j'ai travaillé pour une entreprise classée « secret défense » liée à l'armement. J'étais là pour animer des formations. C'est là que j'ai compris quelle était la vraie faiblesse des entreprises face à l'espionnage. Rien que pour mettre un orteil dans l'entreprise, j'ai dû suivre tout un parcours, y compris être validé par les services de renseignements. Ensuite, j'ai reçu un badge qui m'identifiait comme visiteur et que je devais porter même aux toilettes. Enfin, quelqu'un venait me chercher le matin à l'accueil et j'étais accompagné à chaque déplacement, sans exception. Passer d'un bâtiment à l'autre demandait de badger et le mien n'ouvrait aucune porte, sauf celle du bâtiment de formations. Si je devais changer de bâtiment, je devais demander un accompagnant, qui arrivait toujours très vite et avec le sourire. Car en plus d'être compétents, ces gens étaient sympathiques. Au niveau technique et des procédures, cette entreprise était un exemple car, malgré la lourdeur des procédures de sécurité, le rythme ne s'en ressentait pas trop. La faille était au restaurant de l'entreprise où je mangeais chaque jour. Les gens discutent,

c’est normal, ils rigolent des essais qui ont échoué pour décompresser. Ils se moquent gentiment des clients et expriment leurs espoirs de voir des contrats signés avec tel ou tel pays. Si j’avais été un agent, c’était chaque midi la grande moisson. Le facteur humain est toujours le maillon faible du renseignement et c’est très difficile à changer car l’Europe en général, ne se sent pas très concernée par les menaces d’espionnage.

Un autre point fort de l’écoute passive est si vous êtes à la recherche d’un informateur sur le long terme. Vous travaillez dans une entreprise d’intelligence économique et avoir un fonctionnaire des finances dans votre poche vous serait fort utile. Oui, c’est très mal. Je vous imagine mal vous balader dans les couloirs du ministère avec un panneau « qui veut arrondir ses fins de mois ?». Alors qu’en vous rendant dans les cafés autour du ministère, et en écoutant les conversations, vous identifierez les fonctionnaires les plus démotivés, ceux qui sont en colère parce que « rien ne marche » ou mieux encore, ceux qui se sentent victimes d’une injustice professionnelle. C’est ce profil-là qui est le plus susceptible de trahir son employeur.

L’écoute interactive

L'écoute interactive est une étape de la chaîne où l'auditeur posera des questions, fera écho à certaines des informations qu'il vient d'entendre ou sympathisera avec le sujet pour l'amener à entrer dans les détails. Les questions peuvent être fermées ou ouvertes.

L'écoute interactive n'est à aucun moment hostile, de peur que le sujet ne se taise. La meilleure approche est l'empathie et la compréhension. L'écoute interactive est également libre dans la mesure où la conversation prend la direction que le sujet souhaite prendre. Cette approche permet également à l'opérateur d'établir un rapport avec le sujet, y compris sur ses goûts personnels et ses aversions.

C'est ici que le job se complique car vous devez être bon dans ce que vous faites. Une fois que le stade de l'écoute passive est terminé et que vous avez identifié des cibles potentielles, c'est le moment d'aller au charbon et de prendre contact. Emballer un informateur n'est pas chose facile au niveau personnel car ce sera souvent quelqu'un pour qui vous ne ressentez aucune sympathie et il est même possible que ses propos vous heurtent. Tant pis, gardez vos sentiments pour vous.

Bien entendu, essayer d'emballer un fonctionnaire des finances n'est pas du même niveau de risque qu'avec un ingénieur de la NASA. Si le fonctionnaire vous détecte, ou si vous avez mal calculé votre coup et lui faites une proposition qu'il décline, ce sera sans grande conséquence. Il ne fera probablement rien, ne vous dénoncera pas et vous vous en tirerez avec un simple « non merci ». Avec des cibles d'un haut niveau stratégique, c'est la case prison. Quand je faisais de la recherche de personnes disparues, il m'arrivait parfois d'avoir besoin de l'aide de la police, ce qui est strictement interdit en Belgique. Je faisais simple : je rentrais dans un commissariat et demandais ce dont j'avais besoin en toute transparence. Je n'ai jamais fait ça pour une histoire de mari jaloux, mais dans le cadre d'un rapt parental, oui. Et pas qu'une fois. Un rapt parental n'est pas

une priorité pour la police car l'enfant n'est pas en danger. Donc, il arrive que la famille confie l'enquête à un privé. Quand j'arrive dans un commissariat avec ce genre d'histoire, que pensez-vous qu'un policier fasse ? Il m'aide en prenant des risques. Pour lui, pas pour moi. La moitié des policiers acceptaient. Ceux qui refusaient prenaient toujours le temps de m'expliquer pourquoi et très souvent, c'était parce qu'ils s'étaient déjà fait taper sur les doigts par la hiérarchie dans une histoire similaire. Pas de scandale, pas de dénonciation au Ministère de l'Intérieur ni de menottes.

L'interview

La particularité de l'interview est que le sujet est bien conscient qu'on lui pose des questions, avec les réponses qu'on attend de lui. Vous ne pouvez pas débarquer dans le bureau du directeur général de votre principal concurrent pour lui poser des questions.

Il vous faut un statut. Ou ce que les espions au service de nos beaux pays appellent une légende ou une couverture. Contrairement à l'officier de renseignement qui doit avoir une couverture totale sur tous les aspects de sa vie, vous n'aurez à mentir que sur une partie, plus ou moins importante. De toute façon, si vous êtes démasqué, les conséquences ne seront pas comparables à celles vécues par un agent quand la police iranienne vient l'arrêter à 03H du matin.

Nous allons voir quelques jobs où vous seriez légitime de poser des questions à votre cible.

Le faux cabinet de recrutement

Ici, on entre vraiment dans le cadre d'une opération d'espionnage élaborée, quoi qu'encore simple à réaliser, surtout dans nos pays où la paranoïa industrielle n'est pas de rigueur.

S'il y a bien un endroit où tout le monde parle, c'est bien lors d'un entretien de sélection.

Je suis bien placé pour le savoir, car avant de pratiquer ce si beau métier, je recrutais pour le compte des plus belles compagnies et j'ai à peu près 5000 entretiens de sélection au compteur. Bon, après cette digression autobiographique parfaitement inutile mais délicieuse pour mon ego (comme tout le monde, j'aime parler de moi), passons au boulot.

Vous n'utiliserez cette méthode louche et totalement illégale qu'en situation extrême, vous devez être sérieusement menacé pour l'employer. Ou vous voulez vraiment en apprendre sur votre cible.

Donc, tout le monde parle. Pas sous la torture (je n'en sais rien, je n'ai jamais essayé), pas sous la contrainte, mais volontairement. Les humains sont ainsi faits que chez tous, leur sujet de conversation préféré est eux-mêmes. Ne cherchez pas une exception, n'imaginez même pas une seconde que vous en êtes une, TOUT LE MONDE j'ai dit.

Les étapes à respecter sont :

- Que voulez-vous savoir ? Pourquoi ? Un scénario aussi complexe est-il une façon efficace d'arriver à vos fins ? Non, vous n'improviserez pas. Au

contraire, vous prendrez soin de rédiger un guide d'entretien.

- Qui est votre cible ? Aujourd'hui, le nom de n'importe quel cadre se trouve en deux minutes sur LinkedIn ou Facebook. Sinon, et ça va aussi vite, téléphonez à l'entreprise en disant que vous avez un mail à envoyer au directeur financier, « puis-je avoir son nom, s'il vous plait ?».

- Une fois que vous avez le nom de votre cible, vous devez créer votre personnage. Heureusement, votre légende n'a pas besoin d'être trop complexe. Elle doit impérativement comprendre :

  Un faux nom pour vous. Attention de bien choisir votre nom. Le « candidat » risque de faire une recherche rapide sur les réseaux sociaux. Forcément, il ne vous trouvera pas. Que vous ne soyez pas sur Facebook, passe encore. Mais un recruteur qui serait absent de LinkedIn, c'est peu crédible. Votre nom doit donc être associé à un profil LinkedIn. Soit parce que vous créez un profil, soit parce que vous l'empruntez à un vrai recruteur.

  Le nom d'un cabinet de recrutement, idéalement un cabinet existant à l'étranger, au cas où le « candidat » vérifierait sur le net, ce qu'il fera certainement.

  Un téléphone avec carte, car vous devrez bien lui donner un numéro de téléphone pour vous joindre. Attention qu'il n'est plus facile d'avoir un téléphone anonyme, vous devrez déclarer votre identité. Voir à

ce sujet le paragraphe consacré aux téléphones anonymes.

La carte de visite n'étant plus très tendance, vous pouvez vous en dispenser.

Le nom d'une entreprise pour laquelle vous chassez. Elle aussi, située à l'étranger, mais l'entreprise recrute pour le pays de la cible sinon la personne risque de ne pas vouloir venir à l'entretien, ainsi qu'un profil du candidat idéal, et bien entendu, un job description et un volet rémunérations particulièrement attractif, et réaliste.

Voilà, tout est prêt. Vous avez votre légende. Vous connaissez le nom de votre cible. Il n'y a plus qu'à appâter. N'oubliez pas que vous n'avez rien à vendre. Quand vous contactez la cible, vous devez bien entendu être aimable, mais surtout sobre. Ne vous placez pas en position de demandeur, vous seriez immédiatement traité comme tel. Un chasseur de tête est toujours bien accueilli par un candidat potentiel. Peu importe que le job l'intéresse ou pas, il sera flatté. Si vous donnez le sentiment de vouloir forcer un rendez-vous, la cible se méfiera.

L'étape suivante, vous contactez la cible par téléphone :

« Bonjour, Philippe Delval, du cabinet Human Research International, je travaille pour un cabinet de recrutement américain (ou suisse ou biélorusse), je ne vous dérange pas ? »

Et c'est parti. Le reste, c'est du bon sens.

Au téléphone, vous ne citez pas le nom de votre « client », les vrais chasseurs de tête ne le font qu'au premier entretien en face à face. Vous ne parlez pas non plus de rémunération. En revanche, vous faites miroiter une fonction largement supérieure à celle de votre cible. Le lieu du rendez-vous sera le lobby d'un hôtel chic. Ce n'est pas inhabituel.

Lors du rendez-vous, vous serez sobre, correct, mais ni chaleureux ni sympa. Vous commencerez par poser des questions générales et sans intérêt avant d'aborder les sujets qui vous intéressent vraiment. Il est possible que la cible se réfugie derrière le sceau de la confidentialité pour ne pas répondre à certaines questions, ce qui signifie que vous avez foiré.

Et si la cible se rend compte qu'elle a été piégée ? En principe, ce n'est pas grave, car elle n'osera probablement pas en parler, surtout si ce bon directeur financier a eu la langue bien pendue. Le risque existe, très faible, qu'une plainte soit déposée. J'espère alors pour vous que vous avez bien tout nettoyé derrière vous.

Et là, j'arrive au dernier point: le talent. Si vous n'avez aucun talent d'acteur, que vous ne connaissez rien au monde du recrutement, laissez tomber, vous n'y arriverez pas. De plus, sous-traiter ce genre de mission est difficile car tout ça est fort illégal. Quoi que la ruse soit un moyen légal (en Belgique) pour obtenir de l'information. Peut-être risquez-vous d'être attaqué pour abus de confiance, mais j'ai comme un gros doute.

De toute façon, si cette technique vous plait et que vous l'utilisez, c'est que vous avez le vice dans le sang. Alors, le

droit ou pas le droit ne vous concerne plus, car vous êtes passé de l'autre côté du miroir. Bienvenue.

Le faux journaliste

Le faux journaliste utilise en gros les mêmes outils et attitudes que le faux cabinet de recrutement. Sauf que la légende est plus facile à créer. En gros, vous avez juste besoin de téléphoner à votre cible en disant que vous préparez un article pour tel ou tel média et que vous voulez interviewer la cible. Vous jouez sur la vanité et c'est plutôt rare que ça ne marche pas.

Franchement, vous, si un journaliste vous contacte pour une interview, vous allez réagir comment ? Bon, on est d'accord. Vanité, tout est vanité. Vous pouvez utiliser le nom d'un vrai journaliste au cas où la cible vérifie, ce qui est hautement improbable, mais il y a un risque que la cible découvre que ce journaliste n'a pas du tout l'intention de vous interviewer. Mieux vaut utiliser un nom bidon, ce qui fait toujours un délit en moins, et au cas où la cible vérifie, dire que vous êtes journaliste free-lance.

Comme vous êtes vraiment quelqu'un de prévoyant, vous prenez la précaution de vous acheter une fausse carte de presse sur le net mais personne ne vous la demandera jamais.

https://www.idcreator.com/ se fera un plaisir de vous fabriquer des faux plus vrais que nature, à des prix dérisoires.

La méthode est simple et facile à mettre en place, bien plus que la précédente. Un souci avec le scénario du journaliste, c'est que la télé nous a appris à nous méfier de la presse. Autant un cadre un peu frustré, ils le sont souvent, parlera tranquillement lors d'un entretien de recrutement, autant il sera prudent avec un journaliste, puisqu'il sait que ce qu'il va raconter sera publié. Donc, oubliez les secrets de fabrication et autres projets de fusion/acquisition.

Le faux client

Ce scénario espion est très vaste. Il dépend à la fois de ce que vous voulez savoir et du contexte de votre cible. Nous allons donc en voir une série d'applications et leurs méthodes respectives.

Le mystery shopping est un outil marketing très à la mode ces dernières années. Il s'agit d'envoyer un faux client évaluer vos propres prestations, que ce soit celles des commerciaux de terrain (vendeurs en magasin surtout), soit l'accueil téléphonique. Dans cette version, il s'agit de s'espionner soi-même afin de tester les compétences de ses collaborateurs. TOUTES les entreprises qui y font appel préviennent leurs salariés que cette opération va se dérouler. D'une part pour éviter les problèmes avec les syndicats, et aussi parce que se sachant sur le point d'être évalués, les

salariés donnent durant cette période, le meilleur d'eux-mêmes. Il s'agit ici à la fois d'un outil de renseignement et de management.

J'ai mené une mission de ce type pour un client propriétaire d'une chaine de magasins de vêtements haut de gamme. Les résultats ont été lamentables dans presque tous les magasins. Accueil inexistant, personnel scotché à leur portable, aucune écoute du client, …tout était mauvais sur toute la ligne. D'abord fou-furieux, le client a organisé une réunion avec tout le personnel, décrivant sobrement les résultats magasin par magasin. J'ai vu plusieurs employées se mettre à pleurer. Le client est resté calme, ne s'est pas emporté face au personnel, n'a proféré aucune menace. Trois plus tard, nous avons recommencé l'opération, pas avec les mêmes faux clients évidemment, et les résultats furent spectaculaires en termes de progression.

Le mystery shopping peut et devrait aussi être utilisé avec vos partenaires commerciaux, afin de vérifier que votre distributeur ne raconte pas d'âneries sur vos produits. Et aussi afin de savoir si ce distributeur est efficace dans la commercialisation de vos produits. Par exemple, est ce que votre distributeur parle spontanément de vos produits lorsqu'un client cherche quelque chose proche de votre gamme ?

Ce que je vous suggère, pour enrichir l'information, c'est de mener le même mystery chez vous que chez le concurrent et de comparer les résultats. Le niveau le plus basique du scénario de faux client, c'est encore d'appeler la cible par téléphone pour lui poser des questions.

Dans le cadre de ce guide, il s'agit toujours d'envoyer un faux client, mais cette fois ci vous l'envoyez chez vos concurrents. Avec, encore une fois, un bon scénario travaillé à l'avance.

Ce que vous pouvez apprendre lors de cette mission est proche de ce que vous pouvez obtenir sur un salon, la réactivité de l'équipe interne en plus.

Il y a des situations où cette méthode est relativement facile à utiliser. Lorsque votre concurrent :

- Vend ses produits ou services via des magasins accessibles au public.
- Vend ses produits ou services au particulier.

S'il est facile d'aller étudier votre concurrent vendeur de cuisines équipées ou de salons en cuir, il est beaucoup de métiers où la tradition suppose le déplacement du commercial : piscines, vérandas, châssis…Ici, vous utiliserez le domicile d'une connaissance ou de l'un de vos commerciaux et ferez venir vos concurrents un par un. En quelques jours, vous connaitrez absolument tout des atouts et faiblesses de vos compétiteurs, tant dans le domaine technique qu'humain. Un de mes clients préférés a ainsi constitué un book parfaitement documenté, remis à jour chaque année, dont chacun de ses commerciaux recevait un exemplaire.

Dans le cas où votre concurrent travaille dans le B2B, on peut supposer que ses commerciaux ont l'habitude de visiter les clients dans leur entreprise. Comme il est peu envisageable de faire venir les commerciaux de la

concurrence chez vous, il faut bien trouver autre chose. En gros, vous avez trois options :

I Soit vous trouvez une idée crédible vous permettant de recevoir ce commercial dans un endroit public, un hôtel par exemple, mais si c'est trop inhabituel dans votre secteur, le vendeur se méfiera.

II Soit vous utilisez l'entreprise de quelqu'un d'autre, un ami ou un client (à qui vous ferez un petit cadeau, ça entretient l'amitié) pour recevoir le commercial.

III Soit vous expliquez au commercial que vous préférez venir dans ses locaux, afin de voir à qui vous avez affaire.

Parfois, le boulot peut se faire simplement par téléphone, surtout si tout ce que vous voulez, c'est recevoir une offre. Dans ce cas-là, si on est dans le B2B, vous n'avez pas trop le choix, vous aurez besoin de la complicité d'une personne travaillant dans une autre entreprise, qui recevra l'offre sans éveiller l'attention.

Jusqu'à un certain niveau, c'est très facile et ne demande pas de grande compétence d'investigateur. Le sommet du scénario du faux client est de parvenir à se faire inviter pour une visite guidée des installations du concurrent.

Je n'ai jamais pratiqué le scénario suivant, tout simplement parce que je n'en avais pas besoin. Mais un collègue et ami l'utilisait régulièrement car il était spécialisé dans les intrusions physiques. Ses clients le payaient pour tester leur niveau de sécurité. Il pouvait s'en donner à cœur joie puisque s'il était pris, il ne risquait rien du tout. Il avait comme ça toute une série de selfies de la victoire où il se

prenait en photo dans le bureau du directeur général de l'entreprise qu'il devait tester.

Bref, si vous voulez visiter les installations, les sites de production de votre concurrent, un simple coup de fil ne suffira pas, ni un mail, même bien torché, venant de votre adresse gmail.com.

Prenons un exemple. Votre concurrent est un fabricant de pizzas industrielles. Vous savez qu'il a développé une nouvelle ligne de production qui lui permet de tripler sa capacité. Vous aimeriez bien visiter ses installations tout en sachant qu'une simple demande polie risque de rester sans suite. C'est vital pour vous d'en savoir plus car les prix de votre confrère vont plonger et vous risquez de vous retrouver éjecté de la grande distribution plus vite que dans la « vérité si je mens ».

Vous avez deux options. Soit celle du gros client potentiel, soit celle du fournisseur qui offre une opportunité exceptionnelle. La deuxième option est à la fois plus compliquée et plus aléatoire. Car même si vous proposez du gruyère 30% moins cher, vous n'êtes pas certain d'être invité. Alors que si vous représentez une chaine de distribution hollandaise sur le point de s'implanter en France ou en Suisse, vous serez certainement accueilli à bras ouverts. Et tant qu'à faire, utilisez le nom d'un vrai groupe hollandais.

Il vous faudra cependant un site internet crédible. Vous pouvez en créer un en deux heures avec www.one.com ou www.wix.com. Vous devrez rentrer une adresse mail valide pour vous inscrire. Je vous déconseille d'utiliser une

adresse existante car vous laisserez une trace et aujourd'hui, l'espionnage industriel énerve les autorités. Il pourrait y avoir une enquête. Raison pour laquelle, vous créez une adresse mail sur https://mail.yandex.com/, qui n'est pas intraçable, mais qui complique sévèrement les choses. Sinon, vous pouvez obtenir une adresse email temporaire, anonyme et jetable sur un site comme http://www.yopmail.com/ et cette adresse mail s'autodétruira au bout de quelques jours.

Dans l'idéal, vous conservez le même nom de domaine que le groupe hollandais mais vous l'enregistrez avec un « .fr ». Il y a 9 chances sur 10 que ça ne marche pas car le nom aura certainement été déposé par le groupe hollandais. Mais essayez toujours. Sinon, prenez un nom assez proche et vous écrirez sur votre site « member of XXX group ». Avec votre nouveau site, vous obtenez une adresse email crédible puisqu'au même nom que le site lui-même.

Avant de prendre contact avec la cible, vous aurez pris le temps de rédiger un cahier des charges qui tient la route. Ce doit être faisable puisque c'est votre concurrent.

Ensuite, échanges de mails et coups de téléphone. Vous n'utilisez pas votre téléphone personnel bien sûr, nous avons vu ça dans un autre chapitre. Vous devrez aussi vous munir d'une caméra espion. Le sujet est traité dans le chapitre consacré au matériel.

Ce qui est vraiment délicat dans cette mission, qui jusque-là est plutôt simple à réaliser, c'est le choix de la personne qui fera la visite. Car je ne vous vois pas très bien y aller vous-même. Il faut trouver quelqu'un de très crédible, sûr de lui

et qui « passe » bien avec le chef d'entreprise qui fera sans doute lui-même la visite.

Lorsque j'ai commencé à travailler comme détective privé, j'ai très vite eu beaucoup de succès dans les entreprises. J'aurais bien voulu croire que c'était parce que mes compétences étaient largement supérieures à celles de mes confrères, mais ça n'est pas du tout le cas. En réalité, dans mes débuts, j'étais probablement bien moins compétent que la plupart des autres détectives privés. Mais je parlais le même langage qu'eux. Nous étions du même monde et c'est quelque chose de très difficile à imiter. J'avais moi-même dirigé une entreprise pendant 15 ans, cette entreprise était relativement connue, et sans logique aucune, cela suffisait à faire de moi un interlocuteur crédible pour mener des enquêtes. Dans ce scénario d' « intrusion », la crédibilité sera le facteur déterminant. Cette crédibilité passera par la maitrise de votre personnage, mais aussi par les questions que vous allez poser. Votre attitude aussi. Les acheteurs de la grande distribution ne sont pas connus internationalement pour leur bonté d'âme. Enfin, vous devrez au préalable vous entraîner à utiliser votre caméra pour que ne soyez pas amené à devoir la manipuler durant la visite.

Après la visite, vous avez deux possibilités. Soit, vous cessez simplement de répondre aux mails de l'industriel et il prendra ça comme un manque d'intérêt dans la collaboration. Soit, vous fermez le site et effacez toutes les traces. Dans le premier cas, l'inconvénient est que le site reste en ligne trop longtemps et que l'authentique société hollandaise en soit informée. Dans le deuxième cas, votre pigeon saura qu'il s'est fait avoir et déposera peut-être plainte. Probablement.

Il reste encore une autre façon de pouvoir entrer dans l'usine, c'est de vous y faire engager comme intérimaire. C'est la solution parfaite car la moins risquée et la moins engageante, mais combien de temps avant qu'un poste se libère ?

Le cabinet de notaires

A l'époque où je pratiquais principalement la recherche de personnes disparues, je considérais que c'était mon job de chercher jusqu'à ce que je trouve. J'étais exclusivement dans une logique de chasseur, ce qui je l'avoue, correspond assez bien à mon tempérament. Mais cette logique, aussi exaltante soit-elle, est dévoreuse de temps et d'énergie. Par hasard, je suis tombé sur un article américain à propos d'une opération du FBI. Ils ont envoyé à des milliers d'américains recherchés par la justice, un billet pour une semaine gratuite sur un bateau de croisières. Le prix était envoyé au domicile des personnes recherchées ou à leur famille. La majorité des fugitifs ne se sont pas présentés au port, mais plusieurs centaines d'entre eux sont montés sur l'authentique bateau prévu à cet effet. Ça m'a fait penser que la ruse coutait moins cher que la chasse et j'ai commencé à cogiter sur comment faire venir à moi des gens qui, à priori, n'avaient pas du tout envie de me parler et encore moins de me voir.

J'ai commencé à régulièrement approcher la famille de mes cibles en affirmant travailler pour le cabinet du notaire Machin et qu'il fallait que je puisse parler à Mr Cible ou au moins avoir une adresse officielle car j'avais des documents très importants à lui remettre. Je n'ai jamais dit qu'il y avait

un gros héritage à la clé. C'était inutile. Autant nous associons le mot « huissier » à « emmerdements à venir », autant le mot « notaire » va s'associer librement à de substantiels gains à venir. Bien entendu, les gens me posaient des questions au téléphone, et à chaque fois je répondais que c'est confidentiel, que je ne peux en parler qu'avec Mr Cible, « mais que vous vous doutez bien que si un cabinet de notaire appelle… » sans jamais terminer ma phrase. L'imagination est toujours plus forte que l'argumentation.

Je tiens à préciser que je ne traquais pas des criminels. J'étais soit dans le cadre d'histoires familiales, soit dans la recherche de débiteurs indélicats. Pas des gens qui se méfient de leur ombre.

Le scénario du notaire a fait un carton. Il a juste un inconvénient, il est totalement illégal. J'évitais de tomber dans l'usurpation d'un titre protégé en disant que je travaillais dans un cabinet notarial. Je n'ai jamais dit que j'étais notaire. J'ignore ce que je risquais, je n'ai jamais été inquiété.

Le faux candidat

Ce scénario est le plus mauvais. Voilà, c'est dit. Si votre cible recrute, il est très facile de proposer le cv parfait pour être invité à un entretien de sélection. Mais si c'est pour un poste haut de gamme, vous n'obtiendrez aucune information puisque vous serez certainement interviewé par un recruteur professionnel qui sera bien incapable de vous fournir des informations conséquentes. Si le recrutement est mené directement par votre cible, vous pourrez peut-être obtenir quelque chose puisque dans ce type d'entretien, le

recruteur parle 80% du temps. Mais je trouve que c'est dépenser beaucoup d'énergie pour pas grand-chose. Je le cite quand même parce que en fait, la limite dans le renseignement humain, c'est votre imagination et votre capacité à l'organiser.

La ruse est une méthode d'investigation très limite au niveau légal. Inventer une identité n'est pas une usurpation d'identité, mais se faire passer pour une autre personne en empruntant son nom ou pire, une identité officielle, en est bien une. Sans parler de l'abus de confiance.

Je ne suis pas un moraliste, je le répète, à vous de placer la limite. Pour info, même si je ne suis pas un saint, je n'ai jamais pris une fausse identité officielle. C'est trop dangereux, trop risqué. Et inutile.

2. Détecter le mensonge

En matière de renseignement humain, la détection du mensonge est une arme à haute valeur ajoutée. Tout le monde ment. Parfois pour protéger l'intégrité d'autrui (« mais qu'est ce que tu racontes, ce pantalon ne te grossit pas du tout. ») et donc, ce sont des mensonges mineurs. Les mensonges de niveau intermédiaires sont ceux qui sont émis dans le but d'obtenir un avantage tandis que le niveau le plus grave consiste à couvrir des crimes et des délits.

Beaucoup de gens sont convaincus qu'on ne peut pas le leur faire à eux, qu'ils repèrent les menteurs à 10 mètres mais en réalité, sont étonnamment mauvais pour détecter les mensonges. Une étude, par exemple, a montré que les gens

ne pouvaient détecter le mensonge avec précision que 54% du temps dans un laboratoire - ce qui est impressionnant si l'on tient compte du fait que le taux de détection est de 50% par pur hasard. Comme je ne me souviens plus de la taille de l'échantillon, il est même envisageable que les 4% soient juste la marge d'erreur.

Comme je suis un partisan du moindre effort, je me suis intéressé depuis plus de 20 ans aux aspects technologiques de la détection du mensonge. En effet, si une machine peut faire le boulot, pourquoi se fatiguer à développer des compétences ? La technologie existe, et elle n'est même pas nouvelle. Elle s'améliore même chaque année. Vous trouvez aujourd'hui des tas d'app qui s'installent en un clin d'œil sur votre téléphone.

Le polygraphe a été inventé il y a plus de 100 ans. Quoi de plus logique que d'imaginer que mentir provoque un excès de sudation qui peut être mesuré ? Mais il arrive que le polygraphe soit trompé par plusieurs facteurs. La prise de calmant, se mordre la langue pendant le testing ou plus simplement, vivre une période troublée qui nous place dans une situation de stress non mesurable.

Le Eyedetect de la société Converus est un instrument qui semble largement fiable. EyeDetect mesure les changements dans le diamètre de la pupille, les mouvements des yeux, le comportement de lecture, les clignements…

Mais qu'il s'agisse d'app (surtout utilisées pour faire des blagues), du polygraphe ou de n'importe quel outil de mesure, il s'agit à chaque fois d'avoir l'accord du répondant. Or, le lecteur de ce livre, quel que soit son

métier, travaille dans le renseignement privé, là où vous n'avez aucune autorité sur la personne auditionnée. Vous ne pouvez pas facilement demander à une personne de se connecter à une machine, quoi que cela se fasse dans certains recrutements dans le domaine de la sécurité. Mais je me vois mal demander au futur directeur marketing Europe d'un grand groupe de l'agroalimentaire de se soumettre à ce genre de chose. Il refusera.

Pareil pour un détective privé qui pose des questions à quelqu'un qui peut le mener sur une piste, ou mieux encore, un dirigeant d'entreprise qui pose des questions au commercial de son concurrent pour lui soutirer des informations.

Un professionnel du renseignement doit avoir un bon niveau en analyse du comportement non-verbal. Ce qui m'inquiète, c'est que certains pensent que c'est juste de la connerie. En général, ce sont ceux qui ne se sont pas trop penchés sur le sujet. Donc, cela s'apprend. La bonne nouvelle, c'est que ça s'apprend assez vite. De quelques jours à quelques semaines pour arriver à un niveau tout à faite honorable et acquérir des compétences qui vous feront frimer dans les cocktails les plus raffinés.

Pourquoi l'apprentissage est-il rapide ? Parce qu'il s'agit d'acquérir une nouvelle compétence ET PAS d'en remplacer une. Je m'en suis aperçu quand j'ai commencé à animer ce genre de formation pour une grande banque, pour des avocats et des enquêteurs privés. A la fin d'une simple journée, la progression de l'ensemble des participants était phénoménale. Alors que lorsque j'animais des formations en techniques d'interviews non-directives, les résultats était

nettement moins probants. Tout le monde pense savoir écouter.

Mais y arriver sans :

- Interrompre son interlocuteur
- Poser des questions fermées mais principalement des questions ouvertes
- Porter de jugement
- Donner son avis
- Donner de conseils (qu'absolument personne ne suit jamais)
- Parler de soi
- Négliger de faire preuve d'empathie et être capable de reformuler pour montrer sa compréhension

C'est compliqué parce que ça n'est pas naturel chez la plupart des gens. Les participants étaient bien d'accord pour dire que, oui, une écoute véritable reprend ces critères, mais ils avaient presque tous l'habitude de faire autrement. Dans ce cas, mon cours était un réapprentissage.

Existe-t-il des techniques permettant de détecter le mensonge à coup sûr ? Non.

Maintenant que cela est dit, avançons un peu. Une dernière chose : beaucoup de gens mal instruits de l'analyse du comportement non verbal font la même erreur. Ce que les psychologues appellent le biais de surattribution. Cela veut dire tirer des conclusions larges à partir de l'observation

d’un seul phénomène. Pour faire simple, ça n’est pas parce que quelqu’un croise les bras qu’il faut en arriver à la conclusion que la personne se ferme. Une convergence d’éléments est indispensable.

A) Détecter le mensonge par les méthodes verbales et le questionnement

Dans l'idéal, vous devriez pouvoir voir tout le corps de la personne et ne pas être assis derrière un bureau où une grande partie du corps est caché.

Pendant les interrogatoires, les professionnels qui le peuvent placent souvent le sujet sur une chaise au milieu de la pièce afin de pouvoir rechercher des indices de comportements non-verbaux trompeurs. Bien entendu, vous ne voulez pas donner l'impression d'interroger la personne, mais il est souvent préférable de ne pas avoir d'objet tel qu'un bureau ou une table entre vous et l'autre personne ou de vous asseoir dans un endroit neutre où vous pouvez observer l'ensemble du langage corporel de l'autre personne, par exemple sur un canapé, qui est confortable, relaxant, et qui vous permet de voir l’ensemble du corps de la personne.

Lorsque vous posez des questions à un menteur présumé, il y a des indices verbaux que beaucoup de menteurs révèlent. Voici comment savoir si quelqu'un vous ment en repérant 7 indices de tromperie verbale.

1. Ils répètent votre question avant de répondre - C'est une tactique de blocage courante que les menteurs utilisent pour remplir l'espace mort, tandis que leur esprit tente de

formuler une réponse cohérente avec ce qu'ils ont dit précédemment.

2. Ils répondent par une question de type "brouillard" - Une question de type "brouillard" consiste à vous poser une question en retour. Un exemple pourrait être "Pourquoi me posez-vous cette question ? » ou « pourquoi me demandez-vous ça ? »

3. Répondre de façon culpabilisante et agressive. Un exemple de déclaration culpabilisante est de dire quelque chose comme "Est-ce que vous interrogez tout le monde ? » « Vous pensez vraiment que je serais capable de… ?». Si le phénomène s'accompagne d'une hausse de l'agressivité, il s'agit là d'un fort indice de mensonge. L'image caricaturale est celle de l'homme suspecté par sa femme de tromperie et qui s'emporte à coups de « tu crois vraiment que je serais capable de te faire ça ? » car un homme qui ne trompe pas sa femme cherchera plutôt à la rassurer.

4. Répondre par une justification. La personne ne répond pas à la question mais explique pourquoi elle ne pourrait pas être capable d'avoir fait ce dont vous la soupçonnez. La justification est une explication que personne n'a demandé. Le principe de justification peut s'utiliser pour retourner un menteur. Il y a très longtemps de cela, j'avais lu une recherche australienne en criminologie. Cette étude mettait en avant un effet intéressant du mécanisme de projection. Lorsque les policiers demandaient aux suspects d'un vol « d'après vous, on devrait faire quoi à la personne qui a cambriolé la maison ?», les coupables trouvaient des circonstances atténuantes et se plaçaient en mode empathique. Alors que les sujets innocents disaient presque

toujours que les voleurs devaient être sévèrement punis. Bref, si vous soupçonnez quelqu'un de quelque chose, posez-lui cette question. C'est un truc que j'utilise depuis de longues années et souvent, dans ma tête, je remercie la police australienne.

5.Répondre avec trop de détails. Lorsqu'une personne pense que vous la soupçonnez de mentir, elle essaiera toujours de vous donner la meilleure réponse qui corroborera son histoire. Cela demande beaucoup d'énergie mentale. Cependant, lorsqu'une personne ment, elle exagère souvent son histoire dans l'espoir qu'en fournissant plus de détails, elle prouvera que ce qu'elle dit est en fait vrai.

6. Répondre par des déclarations de distanciation - Une déclaration de distanciation utilise des pronoms plutôt que le nom d'une personne. Considérez la déclaration faite par le Président Bill Clinton lorsqu'il a dit "Je n'ai jamais eu de relations sexuelles avec cette femme". En utilisant "cette femme" au lieu du nom de Monica Lewinski dans la déclaration initiale, Bill Clinton prenait ses distances. Les menteurs ont tendance à prendre leurs distances en supprimant le "je" ou en n'utilisant pas le nom d'une personne spécifique dans leurs réponses. L'utilisation de déclarations de distanciation est souvent une indication qu'une personne pourrait mentir sur quelque chose.

Une autre forme de distanciation est de répondre en termes de valeurs plutôt que sur un fait précis. Dire « je ne volerais jamais le tronc d'une église » n'a pas le même sens que « je n'ai pas volé le tronc de cette église ».

7. Une histoire a un préambule, un événement principal et un épilogue. Lorsque quelqu'un ne passe que peu de temps à

parler de l'événement principal, comme le vol de biens ou la falsification de données, et passe plus de temps à parler des éléments du préambule qui ont conduit à l'événement, cela peut être un indice qu'il ment.

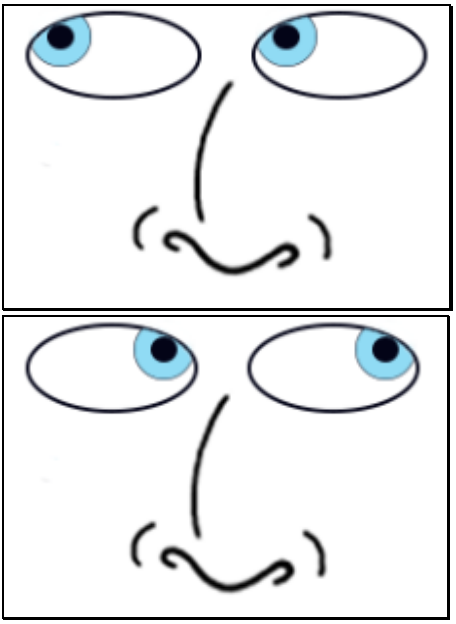
Un autre indice utilisé pour savoir si quelqu'un ment est que les menteurs racontent leur histoire dans l'ordre chronologique, alors qu'à l'inverse, les personnes sincères parlent généralement de la partie la plus intense en premier. Ce n'est qu'ensuite qu'ils complètent l'histoire avec des détails à l'appui.

Pour faire trébucher un menteur présumé après qu'il vous a raconté son histoire, demandez-lui ce qui s'est passé juste "avant" quelque chose, car ce genre de question brise l'ordre chronologique et il est plus difficile pour un menteur de garder le cap. En effet, le mensonge est un bloc compact, contrairement à la réalité. Ce truc est génial en entretien de sélection. Il s'agit de laisser le candidat parler sans l'interrompre avant de lui demander quelque chose comme « et avant votre départ de chez X, que s'est-il passé ? » et vous verrez immédiatement des gens s'embrouiller car une histoire fabriquée ne se raconte pas en arrière. Juste un petit problème neurologique.

Dans le cas du mari suspect de tromperie, ce serait lui demander de raconter sa soirée à partir de maintenant jusqu'au début de la soirée. Mais vous savez déjà qu'il va s'énerver, et s'enfoncer encore plus.

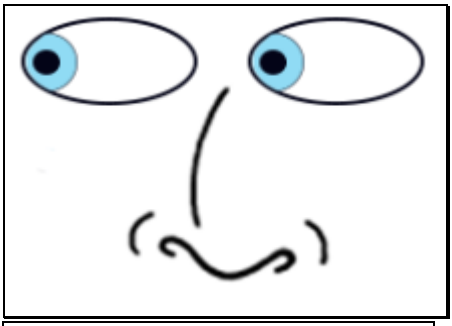
B) Détecter le mensonge par les mouvements oculaires

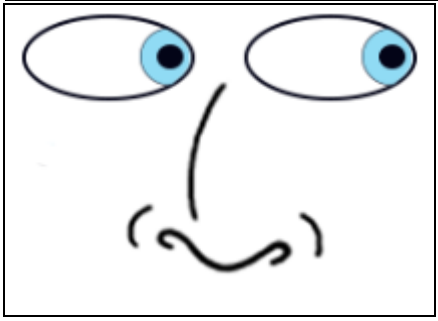
Lorsque nous répondons à des questions, nous allons chercher la réponse dans notre mémoire et cela se voit dans le mouvement des yeux. Ces mouvements oculaires sont différents en fonction du type d'informations que vous allez rechercher dans votre mémoire. A partir de ce fait facile à établir et vérifier, beaucoup de gens en sont arrivés à la conclusion que l'observation du balayage oculaire était une fantastique technique de détection du mensonge. Malheureusement, ça n'est pas aussi vrai que ça. Disons que ça n'est pas faux, mais en faire, comme le prétend la PNL (programmation neurolinguistique), un outil absolu est totalement absurde.



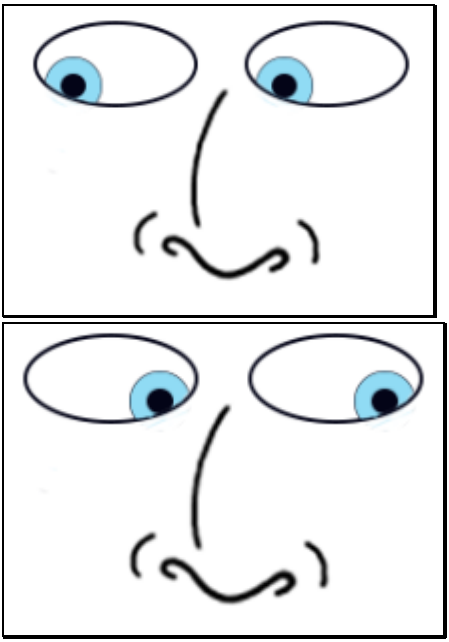
Lorsque'une personne regarde en haut à droite avant de répondre à une question, LA PLUPART DU TEMPS, c'est parce que cette personne va chercher une réponse visuelle construite dans son imaginaire. C'est ce qui a été associé à une réponse mensongère et c'est probablement souvent vrai, mais pas TOUJOURS. Le renseignement est affaire de gens subtils et les généralités à deux balles ne feront jamais de vous un espion d'élite.

Vous pouvez observer que souvent, quand une personne regarde en haut à gauche avant de répondre, elle est en train de fouiller sa mémoire visuelle et donc de se souvenir d'images inscrites dans ses souvenirs et c'est ce qui a été associé à la vérité.





Une personne dont le regard part en balayage latéral droit est en création de sons ou de bruits. C'est dans son imaginaire. Testez le sur vous, et immédiatement vous vous rendrez compte que vos yeux ne partent pas dans la même direction lorsque vous vous souvenez d'une chanson et lorsque vous composez vous-même un air. Le balayage latéral vers la gauche est donc associé à la réminiscence de souvenirs auditifs.



Le regard plongeant vers la droite est souvent relié à la création imaginaire de sensations kinesthésiques, c'est-à-dire liées au toucher. A l'inverse, le regard plongeant vers la gauche est lié à des souvenirs kinesthésiques ou à un dialogue interne.

Maitriser cette technique est un bon moyen d'apprendre à détecter certains mensonges, ou en tout cas, d'avoir des éléments qui laissent à penser que mon interlocuteur est ou n'est pas sincère. Cependant, il existe certains biais.

Le premier est que cette espèce de cartographie du regard est très loin d'être une vérité absolue. Ce qui précède est vrai pour la majorité de la population, mais pas pour tout le monde. Cela veut dire que pour être sûr de tirer des conclusions pertinentes, il faudra poser à votre sujet des questions de contrôle, dont vous connaissez la réponse, afin de valider sa cartographie personnelle.

Le deuxième biais est que les personnes non entrainées ont tendance à poser des questions fermées. C'est-à-dire des questions ou les réponses seront de type binaire. Oui ou non, à droite ou à gauche. Pour pouvoir détecter les mouvements oculaires, vous devez absolument poser des questions ouvertes qui nécessitent de la part de votre sujet une authentique recherche dans son disque dur. Si les questions sont fermées ou trop simples, vous ne verrez rien du tout.

Enfin, il est très difficile pour le commun des mortels d'être attentif à une conversation et d'observer attentivement le mouvement des yeux de son sujet. Dans un monde parfait, vous pourriez filmer votre cible de face durant l'entretien afin d'étudier la vidéo par la suite. La clé, c'est l'entrainement et je vous suggère de tester vos proches. Avec parcimonie si vous ne voulez pas, comme cela m'est arrivé, vous retrouver avec votre moitié portant des lunettes de soleil au petit déjeuner.

C) Détecter le mensonge par l'observation du comportement non-verbal

Lundi matin, vous arrivez au boulot et croisez Mathieu. Par réflexe, vous lui demandez s'il a passé un bon weekend et il répond « oui, pas mal » en haussant l'épaule droite. Intuitivement, vous savez qu'il n'a pas passé un excellent weekend. Lorsqu'une personne dit une chose et que simultanément l'épaule droite se soulève, cela veut presque toujours dire que la vérité est à l'exacte opposé des mots prononcés.

Bienvenue dans l'étude des comportements non-verbaux. Il est en effet très facile, vous l'avez fait des milliers de fois, de mentir avec les mots. Mais faire mentir son corps est bien plus compliqué, voire impossible sur un long moment.

Une partie de l'analyse des comportements non-verbaux concerne l'expression des émotions sur le visage du sujet. Il s'agit là d'une partie essentielle des travaux du psychologue Paul Ekman. Celui-ci détermine qu'il existe 8 émotions de base et qu'elles sont universelles et génétiquement déterminées, et donc que la culture a un impact sur la façon d'exprimer ses émotions, mais que globalement, les caractéristiques de base de l'expression d'une émotion sont universelles. Ces émotions sont :

- La peur
- La colère
- La joie
- La tristesse
- Le mépris
- Le dégout
- La surprise

- La honte

Cela ne signifie nullement qu'il n'existe pas d'autres émotions, mais cette courte liste représente les émotions de base, un peu comme il existe les couleurs de base.

L'intérêt pour une personne active dans le renseignement est d'une part d'être capable d'identifier ces émotions via les expressions faciales, et d'autre part, d'identifier ce que Ekman appelle les micro-expressions, qui sont des expressions fugitives et très révélatrices de l'état d'esprit de votre cible.

Pour devenir un champion de l'analyse du comportement non-verbal, il faut deux choses : les compétences pour détecter les signaux, et la rapidité. Les compétences s'acquièrent par l'apprentissage et la rapidité, par l'expérimentation constante.

Vous trouverez sur You Tube une masse de vidéos en français ou en anglais traitant de ce sujet et vous proposant de vous entraîner. Très bien. Le problème est toujours le même : les gens arrivent trop vite à des conclusions. L'observation du comportement non-verbal n'est pas une science absolue. A de rares exceptions près, vous ne pouvez pas associer un comportement observé à une signification absolue.

Les clés ici sont l'humilité et l'apprentissage.

Ma recommandation ici sera de regarder une série américaine. « Lie to me » est une série qui raconte les aventures du Docteur Lightman, dont la mission est de déterminer ce qui est la vérité dans des affaires civiles ou

criminelles. Personnellement, je trouve la série passionnante, mais ce n'est pas ce qui compte. C'est surtout une série où vous allez apprendre énormément de choses sur l'étude des comportements non-verbaux.

D) La technique scintigraphique

Vous dirigez une organisation et vous savez que des informations sensibles sont transmises aux médias. Quelques personnes sont susceptibles d'être responsable de ce manque de discrétion, mais vous ne savez absolument pas qui. Normalement, vous avez confiance en chacun d'eux. La technique scintigraphique est pour vous. La scintigraphie est une méthode d'imagerie médicale. Le patient reçoit une injection d'un traceur radioactif, ce qui permet l'observation d'une tumeur. C'est exactement le même principe ici. Si quatre collaborateurs sont susceptibles d'avoir parlé à la presse, vous leur racontez à chacun la même histoire, sous le sceau du secret, en changeant un détail pour chacun d'eux. Vous pouvez le faire simultanément ou l'un après l'autre. Le faux détail, c'est le traceur. Quand il apparait dans la presse ou sous forme de rumeur, vous tenez votre coupable.

3. Comment inspirer confiance à sa cible

Au moment où j'écris ces lignes, je vis en Thaïlande depuis quelques mois. Il y a quelques jours, je me baladais en ville, et j'entends un homme parler français avec un accent de ma région. Spontanément, je vais vers lui et je lui demande s'il est de Charleroi. Il me fait le sourire de celui qui retrouve son frère après des années d'errance. Deux minutes plus tard, nous sommes attablés devant une bière. Mais si j'avais croisé la même personne dans les rues de ma ville d'origine, rien de tout ça ne serait arrivé.

Oui, bon, et alors ? Et alors, nous nous sentons bien avec les gens avec qui nous avons des points communs. Nous nous sentons bien avec les gens qui nous ressemblent. Encore une fois, il ne s'agit pas d'une affirmation absolue mais d'une tendance. Et une tendance comportementale peut toujours être utilisée à des fins diverses, plus ou moins bienveillantes. La bienveillance n'étant pas précisément le cœur de ce livre, nous allons parler de synchronisation.

La synchronisation est l'art et les techniques qui visent à vous calquer sur votre cible. Cela pourrait aussi s'appeler « l'effet caméléon ».

Il est possible de se synchroniser à différents niveaux. Les très bons communicateurs le font en partie spontanément.

- Sur le langage verbal : parler de la même façon que la cible, adopter des mots communs, avoir le même niveau de langage.
- Sur le langage non-verbal : se positionner comme la cible, bouger comme elle, sans effet caricatural. Si

vous vous grattez le nez parce que votre interlocuteur se gratte le nez, vous allez manquer quelque chose.

- Sur les valeurs : avoir des valeurs communes pousse au rapprochement. A l'opposé, un désaccord sur les valeurs à tendance à éloigner les gens.

- Sur les activités : avoir un hobby commun avec sa cible vous ouvrira le chemin de son affection. Le risque est bien sûr d'être découvert si vous n'y connaissez rien.

- Sur le langage para-verbal : vous parlez au même rythme que votre interlocuteur. Parler plus vite que lui donnera irrationnellement la sensation que vous êtes hautain ou agressif. Parler plus lentement, celle que vous êtes un peu ralenti intellectuellement. Ça, c'est le rythme de l'élocution. Vous vous calquez aussi sur sa hauteur de son.

Cette technique est utilisée par les négociateurs d'élite. Son utilisation a tendance à détendre votre vis-à-vis. On ne parle pas d'hypnose, mais d'une forme de relaxation provoquée. Les champions olympiques de la technique parviennent à se calquer sur le rythme respiratoire de la cible.

La deuxième façon d'inspirer confiance est d'écouter sa cible avec attention. On aime toujours au minimum un petit peu, quelqu'un qui vous écoute beaucoup. Laissez parler la cible, passionnez-vous pour sa misérable carrière, manifestez votre empathie pour toutes les promotions qui ont été proposées à ses collègues bien entendu pistonnés, ne parlez pas de vous, ça ne l'intéresse pas. Rappelez-vous que

vous n’êtes jamais aussi passionnant que quand vous ne dites rien. Ne critiquez jamais les choix ou décisions de votre cible, même si vous avez envie de vomir. Faites-lui sentir qu’il ou elle est la personne la plus intéressante de la terre. Bienvenue dans le « diner de cons » du renseignement.

4. La manipulation au service du renseignement offensif

Le renseignement de source humaine et l’ingénierie sociale ont en commun que le facteur humain est au cœur des opérations. Une chose les distingue cependant : la finalité. Le Humint a pour objectif de collecter de l’information, alors que le but de l’ingénierie sociale est d’attaquer et de manipuler pour obtenir un avantage.

L'ingénierie sociale est le terme utilisé pour un large éventail d'activités malveillantes réalisées par le biais d'interactions humaines. Elle utilise la manipulation psychologique pour tromper les utilisateurs et les amener à commettre des erreurs de sécurité ou à donner des informations sensibles.

Ce qui rend l'ingénierie sociale particulièrement dangereuse, c'est qu'elle repose sur l'erreur humaine, plutôt que sur les vulnérabilités des logiciels et des systèmes d'exploitation. Les erreurs commises par les utilisateurs légitimes sont beaucoup moins prévisibles, ce qui les rend plus difficiles à identifier et à déjouer qu'une intrusion basée sur un logiciel malveillant.

Les attaques d'ingénierie sociale se présentent sous de nombreuses formes différentes et peuvent être effectuées partout où il y a une interaction humaine.

Les pirates de la pensée font un usage prodigieux des faiblesses inhérentes à presque tous les humains : croire que nous sommes meilleurs que les autres (et donc qu'il est inutile d'être prudent) et la façon que nous avons de justifier nos échecs par des facteurs externes et nos réussites par des facteurs internes. En gros, je ne suis responsable que de ce que je réussis. C'est ce que les psychologues appellent le biais de complaisance. L'ingénierie sociale utilise aussi d'autres facteurs psychologiques : le besoin d'aider quelqu'un qui nous le demande car il est très difficile de refuser de donner de l'aide. Mais aussi la soumission à l'autorité qui veut que l'immense majorité de la population obéît à un ordre donné par quelqu'un détenteur d'une autorité considérée comme légitime. L'égo et l'avidité complèteront cette liste.

Le phishing

Le phishing est l'une des attaques les plus populaires en matière d'ingénierie sociale. Il s'agit de campagnes de mailings, de SMS ou de messages venant des réseaux sociaux, visant à créer un sentiment d'urgence, de curiosité ou de peur chez les victimes. Il les incite ensuite à révéler des informations sensibles, à cliquer sur des liens vers des sites web malveillants ou à ouvrir des pièces jointes contenant des logiciels malveillants.

Un exemple est un courrier électronique envoyé aux utilisateurs d'un service en ligne qui les avertit d'une violation de politique exigeant une action immédiate de leur

part, telle qu'un changement de mot de passe obligatoire. Il contient un lien vers un site web illégitime - presque identique en apparence à sa version légitime - qui invite l'utilisateur non averti à entrer ses informations d'identification actuelles et son nouveau mot de passe. Une fois le formulaire soumis, les informations sont envoyées à l'attaquant.

Certaines campagnes sont puériles et pratiquement personne ne tombe dans le panneau. D'autres sont nettement plus élaborées. Et ne sont pas forcément très difficiles à mettre en place. Imaginons que vous ayez un abonnement au site tarata.fr et que vous receviez un mail de tarata.be ou tarata.it ou .eu ou tratata.fr, il y a de bonnes chances que vous n'y voyez que du feu.

Par exemple, je suis propriétaire du nom de domaine agakure.eu, mais je n'ai pas acheté tous les noms de domaines potentiels.

Beaucoup de sites vous permettent de savoir si un nom de domaine est libre.

https://www.ovh.com/fr/domaines/

Les appâts

Comme son nom l'indique, les attaques par appât utilisent une fausse promesse pour piquer la cupidité ou la curiosité d'une victime. Elles attirent les utilisateurs dans un piège qui leur vole leurs informations personnelles ou inflige à leurs systèmes des logiciels malveillants.

La forme d'appât la plus décriée utilise des supports physiques pour disperser les logiciels malveillants. Par exemple, les attaquants laissent l'appât - généralement des clés USB infectées par des logiciels malveillants - dans des endroits bien visibles où les victimes potentielles sont certaines de les voir. L'appât a un aspect authentique, comme une étiquette le présentant comme la liste de paie de l'entreprise.

Les victimes ramassent l'appât par curiosité et l'insèrent dans un ordinateur au travail ou à la maison, ce qui entraîne l'installation automatique de logiciels malveillants sur le système. Les escroqueries à l'appât ne doivent pas nécessairement être réalisées dans le monde physique. Les formes d'appâts en ligne consistent en des publicités attrayantes qui mènent à des sites malveillants ou qui encouragent les utilisateurs à télécharger une application infectée par un logiciel malveillant.

Un exemple vu il y a peu en ligne : un site, visiblement indien, me promet que pour 50 euros, j’aurai un logiciel qui pourra télécharger les adresses mails de LinkedIn, Facebook, et de quelques autres réseaux sociaux. Pour 50 euros, je tenterais bien le coup. Surtout que la démo est alléchante. J’avais déjà ma carte de crédit en main quand je me suis quand même décidé à regarder si le logiciel avait

des commentaires quelque part. Non. Un site Facebook ? Oui, mais visiblement tout neuf et sans commentaire. J'ai rangé ma carte de crédit.

Vous vous dites qu'il faut être un hacker de haut vol pour réussir un truc comme ça. Quand je pense qu'il y a deux jours, alors que je tentais péniblement de monter un ventilateur, ma compagne me regardait avec la compassion amusée que l'on réserve aux enfants maladroits. Evidemment que je ne suis pas capable de fabriquer ce genre de logiciel. Et si j'en utilise un que je trouve sur le web, il sera identifié à coup sûr par n'importe quel antivirus. Mais n'importe quel étudiant en informatique peut le faire, lui.

Le harponnage

Il s'agit d'une version plus ciblée de l'arnaque de phishing, dans laquelle un attaquant choisit des personnes ou des entreprises spécifiques. Ils adaptent ensuite leurs messages en fonction des caractéristiques, des postes et des contacts de leurs victimes afin de rendre leur attaque moins visible. Le harponnage requiert beaucoup plus d'efforts de la part de l'auteur et peut prendre des semaines, voire des mois, pour être mis en place. Un scénario de harponnage peut impliquer un attaquant qui se fait passer pour le consultant informatique d'une organisation et envoie un e-mail à un ou plusieurs employés. Il est rédigé et signé exactement comme le consultant le fait normalement, trompant ainsi les destinataires en leur faisant croire qu'il s'agit d'un message authentique. Le message invite les destinataires à changer leur mot de passe et leur fournit un lien qui les redirige vers

une page où l'attaquant saisit leurs informations d'identification.

Pour envoyer un mail à partir de n'importe quelle adresse, que ce soit celle de votre patron ou de ce consultant en informatique, il suffit de s'inscrire sur une plateforme d'envoi de newsletters. Oui, il faut s'inscrire, mais nous avons vu dans un autre chapitre comment s'inscrire sur un site avec une adresse jetable ou qui s'autodétruit après 10 minutes.

Ces plateformes ont pour mission d'envoyer un message à un nombre conséquent de lecteurs. Pour ça, il faut bien sûr rédiger un texte. Puis il faut aussi uploader une base de données d'emails. Mais ce qui est amusant, c'est quand la plateforme vous demande d'introduire l'adresse d'envoi. Certaines plateformes vous demandent d'introduire l'adresse email en question, puis vous devez aller sur votre messagerie pour bien confirmer qu'il s'agit de votre adresse. Mais certaines plateformes ne le font pas et vous pouvez alors envoyer un mail à partir de l'adresse que vous voulez. Imaginez ce que vous pouvez faire quand vous avez le pouvoir d'écrire n'importe quoi à partir de la messagerie de n'importe qui. La plateforme YMLP vous le permet à ce jour. Je suppose que ça pourrait changer.

https://www.ymlp.com/

http://deadfake.com/ est lui un site dédié à l'envoi de faux emails. Ils disent que c'est uniquement pour faire des blagues. Je ne suis pas certain que tout le monde rigole.

Il y en a beaucoup et vous pouvez utiliser « *how to spoof emails* » comme requête sur Google pour être toujours au

gout du jour. Ces mails sont théoriquement détectables comme étant faux. Mais on s'en aperçoit généralement après.

De toute façon, n'importe quel serveur peut être configuré pour l'envoi d'emails partant de l'adresse de son choix.

Le harponnage peut aussi se faire par téléphone. La seule technique, c'est être le champion du baratin. Une arnaque de ce type a eu beaucoup de succès en France, où un individu se faisait passer pour le PDG de la compagnie, appelait un employé de la compta et faisait pression sur cet employé pour que celui-ci vire une importante somme d'argent en urgence. Cela demande beaucoup de temps pour étudier son rôle, mais aussi le profil de la victime.

Dans ce genre de scénario, il faut être capable de modifier son numéro de téléphone. Un appel en aveugle ne vous ouvrira pas beaucoup de portes car vous commencez le contact en créant de la méfiance.

Le principe de base de l'usurpation de l'identité de l'appelant consiste à modifier les informations affichées sur l'écran d'affichage de la personne appelée. Quelques-uns des points abordés dans ce chapitre indiquent que nous pouvons utiliser l'argument d'autorité et/ou d'engagement pour influencer une personne. Le numéro direct de votre directeur affiché sur votre écran fait monter la crédibilité à son niveau maximum.

Mais l'appelant peut aussi être un collègue d'un autre service, un prestataire de service, un officier de police.

On pourrait croire que cette incroyable technologie n'est réservée qu'à l'élite du renseignement, et ça a été vrai. Mais

ça n'est plus le cas. Aujourd'hui, vous pouvez trouver des sites de « spoof id » n'importe où. Et si vous avez un smartphone, vous trouverez sur https://play.google.com/ des tas d'applications plus ou moins gratuites. « Fake Friend Call » est l'une d'entre elles. Le problème de ces apps est qu'elles sont formidables lundi et ne fonctionnent plus du tout le mardi. Vous avez l'endroit où les trouver, les mots clés, il ne vous reste plus qu'à être qui vous voulez au téléphone. Il existe aussi des transformateurs de voix mais on est là trop dans le gadget pour que j'en parle dans ce livre. Mais on peut imaginer du matériel qui parviendrait à transformer votre voix en celle de quelqu'un que votre cible connait. En fait non, pas besoin de l'imaginer car cela porte un nom, le « deepfake ». Le deepfake est une technologie très récente qui pourrait se résumer à l'art de totalement transformer la réalité sans que cela soit visible. Cela peut se faire au niveau visuel et/ou vocal. Le premier cas dont j'ai entendu parler date seulement de 2019 quand un escroc a réussi à « emprunter » la voix d'un PDG allemand et à détourner une importante somme d'argent.

Le Deepfake audio peut être utilisé à toutes sortes de fins, allant du divertissement aux activités criminelles. La plupart des applications audio Deepfake sont destinées à des fins de divertissement, mais peuvent également être utilisées à des fins plus nuisibles. L'Etat de Californie vient tout juste de légiférer à ce sujet.

Le clonage de voix consiste à prendre un fichier audio de n'importe quelle voix individuelle et à l'utiliser comme source pour créer de faux enregistrements audios. Avec seulement quelques heures de matériel source

(enregistrements audios d'une voix individuelle), le logiciel deepfake audio est capable de cloner la voix afin de l'utiliser. Il n'est pas encore possible de trouver un système qui vous permettrait de modifier votre voix en live, au téléphone, en utilisant la voix d'une personne en particulier. On commence à trouver des logiciels où vous pouvez utiliser des voix de personnes célèbres, et c'est très convaincant ou des applications qui vous permettent de modifier votre voix, mais le clonage en direct n'est pas pour tout de suite. Au rythme où vont les choses, la technologie ne devrait pas tarder à être accessible.

Pour conclure ce chapitre sur l'ingénierie sociale, j'ai une question à vous poser, un petit test :

Imaginez la scène suivante : vous rentrez dans votre immeuble, suivi de près par un homme dans la quarantaine. Il porte un élégant costume bleu et fait mine de vous suivre à l'intérieur de l'immeuble. Vous visualisez la scène ? Elle est relativement banale et quelque chose de similaire a dû vous arriver bien des fois. Que faites-vous ?

a) Vous lui ouvrez la porte avec un grand sourire

b) Vous n'avez pas envie de lui ouvrir la porte mais comme il vous colle de près, vous ne vous sentez pas le courage de lui poser des questions.

c) Vous lui demandez poliment qui il vient visiter.

d) Vous ne demandez rien du tout et lui fermez la porte au nez.

La plupart des gens vont répondre c). Faites le test autour de vous. Ce qui est merveilleux dans le comportement humain,

c’est qu’en réalité, nous sommes incapables de prédire nos propres comportements car ils dépendent beaucoup moins des facteurs inhérents à notre personnalité qu’au contexte d’un évènement.

5. Usurper une adresse mail ou envoyer un mail anonyme

Nous avons vu dans le point précédent qu’il est possible d’envoyer un mail très simplement à partir de l’adresse d’absolument n’importe qui. Si je veux envoyer un message à 100.000 personnes en utilisant l’adresse de Bill Gates, il ne pourra rien y faire. Cette méthode peut bien entendu avoir des effets absolument dévastateurs, mais présente un inconvénient. Vous pouvez envoyer les mails, mais pas recevoir les réponses. Puisque vous n’avez pas accès à la boite de réception. La personne sera informée dans la minute de l’utilisation frauduleuse de son adresse de deux façons : via les réponses qu’il recevra éventuellement, et surtout via les mails qui n’aboutiront pas chez leur destinataire et qui rebondissent avant de laisser un message d’erreur dans la boite de celui qui a envoyé le message. Bien sûr, ici, la cible n’a envoyé aucun message, mais sait maintenant que quelqu’un l’a fait. Il ne peut dans l’immédiat pas faire grand-chose puisqu’il ne sait pas à qui vous avez écrit en son nom.

Il y a d’autres moyens pour envoyer des mails anonymes.

Le plus simple, si vous avez besoin d’un anonymat modéré, est de vous créer une adresse via n’importe quelle messagerie gratuite. Il y en a beaucoup, dans des tas de

pays. Rien de plus simple. Mais ici, votre fournisseur d'adresse peut vous identifier. Soit via les informations données lors de votre inscription, soit via votre adresse IP. Votre cible peut aussi vous identifier via l'en tête du mail où se trouve votre adresse IP.

A ce stade, vous avez deux options : l'utilisation d'un VPN, qui vous garantit que votre IP ne peut être localisée ou faire appel à un « remailer ». En gros, vous n'envoyez pas votre mail à votre cible, mais à un autre serveur qui se charge de l'envoi. Et si vous êtes vraiment anxieux, vous pouvez doubler ou tripler vos remailings. Mais là, on tombe dans la parano totale, ce qui est un risque conséquent quand on travaille dans le renseignement. Une nouvelle adresse chez un fournisseur gratuit, dans un autre pays que le vôtre, accompagné d'un VPN, devrait être largement suffisant. Choisissez un VPN « no log », c'est-à-dire qui ne conserve pas les traces de votre navigation, ni même vos informations personnelles.

Si vous avez besoin d'une adresse pour quelques minutes, https://10minutemail.com/ vous en fournira une qui s'autodétruira au bout de dix minutes. Très utile pour s'inscrire sur un site en toute discrétion.

Vous pouvez aussi utiliser https://temp-mail.org/fr/

6. Faire les poubelles

Si vous n'êtes pas vite dégoûté, vous trouverez beaucoup de renseignements dans les poubelles. Car vous pouvez faire les poubelles de votre concurrent, mais aussi celles des

dirigeants de la compagnie. Dans nos pays où la méfiance est si peu de rigueur, tout finit par se retrouver en déchets, et la plupart du temps sans être passé au préalable par une déchiqueteuse.

Chez un particulier, c'est simple, vous connaîtrez toute sa vie. Toutes ses habitudes. Et très souvent, sa situation financière. Dans une entreprise, ça dépendra de la négligence des dirigeants, souvent très grande chez nous.

Mais en gros, vous y trouverez :

- ébauches de contrats
- Photocopies de cartes de crédit
- Brouillons de plans, analyses, projets en cours ou à venir

Soit les infos trouvées peuvent être utilisées sous forme brute, soit comme préalable à une deuxième étape (si vous découvrez que votre concurrent est sur le point de vendre à un des gros acteurs du marché, c'est le moment d'approfondir vos connaissances sur cet acteur).

Sachez qu'en Belgique, une poubelle se trouvant sur la voie publique…est publique. Ce qui veut dire que vous avez le droit de la fouiller, de la prendre, et que toute information obtenue par ce moyen est considérée comme de l'information publique.

Le mieux à faire pour ce genre de job est de venir en camionnette, de piquer les poubelles et de les ouvrir tranquillement dans un endroit bien aéré.

Même si la méthode est peu ragoutante, elle était une pratique courante chez les détectives privés. Car toutes nos habitudes et bon nombre de nos secrets finissent dans nos poubelles. C'est peut-être moins vrai aujourd'hui puisque bon nombre de nos secrets se trouvent cachés au cœur de nos ordinateurs. En revanche, depuis le tri sélectif, il est tout de même plus agréable de ne se préoccuper que des papiers de notre cible, puisqu'il s'agit de ce qui nous intéresse.

Dans les entreprises, tout se passe sur écran mais nos mœurs ont peu évolué. Nous imprimons toujours beaucoup. Qui dit impression, dit déchets. Dans votre entreprise, les déchets papiers passent bien tous à la déchiqueteuse ?

7. Contacter les clients de la concurrence

Si vous voulez connaître les points forts et les points faibles de votre concurrent, la meilleure chose à faire est encore de le demander aux clients.

Vous pouvez vous contenter de lire les opinions, critiques et autre « reviews » que vous trouverez sur le net. Nous en parlerons. Mais ces commentaires en ligne ont trois inconvénients :

- Cela concerne surtout les entreprises qui vendent au particulier ou le secteur des services. Très peu le secteur industriel.
- Une infime partie des consommateurs se donne la peine de publier un avis.

- Seuls les extrêmes expriment leur opinion. Les très satisfaits et les très insatisfaits.

La méthode à utiliser est simple et peu stressante. Ici, nous sommes dans une démarche de recherche d'informations et pas de prospection. L'idée est de téléphoner à ces entreprises et de dire au responsable que vous envisagez de travailler avec la société X (votre concurrent), mais que vous hésitez.

L'expérience m'a montré que cette démarche est très efficace car les interlocuteurs s'expriment très facilement. Notre égo nous pousse à adorer l'idée que quelqu'un sollicite notre avis, car c'est à la fois très rare et très valorisant. Bien entendu, vous avez pris la précaution de ne pas être identifiable, ce qui se fait, on ne peut plus simplement, en appelant en aveugle d'un téléphone portable. Ensuite, l'acheteur se fera une joie de tout vous raconter sur :

• La qualité du service

• La qualité des produits

• Le service après-vente

• Les délais de livraison

• Et bien sûr, si vous êtes un peu adroit, les prix

Je vous suggère, en fin d'entretien, de poser deux questions ouvertes :

« D'après vous, qu'est ce qui peut être amélioré chez X ? »

« D'après vous, qu'est ce qui marche le mieux chez X ? »

Ces informations sont d'une importance capitale dans une démarche d'analyse concurrentielle. Soit la démarche vous permettra d'identifier un gros point faible chez votre concurrent, et donc de plonger sur sa clientèle, soit c'est chez vous que le point faible sera identifié, et donc vous pouvez l'améliorer.

La technique exposée ici est très simple, très facile à mettre en place, ne demande aucune compétence particulière, ni matériel pointu.

L'une de mes préférées.

8. Les foires et salons

Vos concurrents présentent leurs nouveautés lors de foires et salons. C'est votre boulot de vous y trouver. En tant que manager de la compagnie, c'est plutôt délicat de vous faire passer pour un client sur un salon. Vous risquez d'être reconnu, ce qui est fort embarrassant. Mais il y a pire que l'embarras : si vous êtes reconnu, rien ne dit que l'information reçue sur le stand sera fiable.

Bref, faites appel à l'équipe.

Dans tous les cas, une visite sur salon, comme toute mission de renseignement, doit avoir un ou des buts. Y aller par curiosité est fort sympathique, surtout si vous y allez en famille, mais fort peu professionnel, sauf si vous êtes dans un secteur qui vend au particulier (auquel cas, votre famille peut faire partie du scénario).

Sur un salon professionnel, vous pouvez obtenir de l'info sur:

• Tarification (obtenez une offre)

• Forces et faiblesses de l'équipe de vente

• Innovations techniques

•Délais de livraison, délais de paiement, délais d'intervention

• Identification physique du personnel du concurrent

• Ce que le concurrent pense et dit de votre compagnie

• Ce qui ne va pas chez le concurrent (les vendeurs adorent se plaindre)

Ne vous fiez surtout pas à votre mémoire. Infidèle, elle vous trahira et vous ne retiendrez que ce que vous voulez entendre. Enregistrez tous vos échanges avec un micro à la fois discret et de qualité. La qualité est importante car un salon est un endroit bruyant et vous risquez de tout perdre à cause d'un enregistrement de mauvaise qualité. Ne planquez jamais le micro dans vos vêtements, le froissement du tissu polluera totalement le son. Passez faire un tour dans le chapitre consacré au matériel d'espionnage.

Dans votre pays ou à proximité…

Si c'est simple et sans risque, demandez à un employé de la société ou à un membre de sa famille. Si vous êtes dans un secteur où un acheteur potentiel doit avoir des connaissances techniques, ça se complique. Soit vous

trouvez quelqu'un qui a ces connaissances, soit vous créez un scénario qui explique pourquoi vous ne les avez pas.

Surtout, ne négligez jamais votre crédibilité !

Vous pouvez faire appel à un client, un vrai, en échange de je ne sais pas quoi. Le mieux, ce sont vos commerciaux. Ils vont à la pêche aux infos et c'est directement utilisable sur le terrain. Le problème avec les vendeurs, c'est qu'on dirait qu'ils sont atteints d'une étrange maladie qui les empêche de remonter l'info jusqu'au département marketing. Et surtout, le problème est le même que pour vous, ils risquent fort d'être reconnus. L'expérience montre aussi que les commerciaux ont du mal à comprendre l'intérêt de l'information concurrentielle. Ils répugnent à mener des missions simples de « client mystère », tout en se plaignant que les concurrents soient moins chers et plus évolués techniquement que vous.

Si personne ne peut le faire, demandez à une boite de mystery shopping. Ça ne risque pas de vous ruiner. C'est supposé être leur métier. Mais ça ne règle pas le problème s'il est absolument nécessaire d'avoir de hautes compétences techniques pour être un client crédible dans votre secteur. De plus, les entreprises de mystery shopping se battent beaucoup sur les tarifs. En conséquence de quoi, les clients mystères sont souvent mal payés et donc, le niveau n'y est pas. Une autre solution est de faire appel à une entreprise de formation en techniques de vente. Les formateurs ont l'habitude de ce genre de mission quand il s'agit de travailler dans le haut de gamme. Le tarif s'en ressentira lourdement. Comptez entre 600 et 1.300 euros la journée. Mais vous aurez du beau boulot.

A l'étranger

Là où ça se corse sérieusement, c'est quand vos concurrents bien aimés se présentent sur des salons à l'étranger.

La première option est évidemment d'y aller vous-même. Ça vous fait un petit voyage pas stressant aux frais de la société. Ça fait cher, juste pour espionner un concurrent sur un salon à l'autre bout du monde. Mais si la société n'envisage pas de vous payer des vacances, un autre système devra être envisagé. Système que nous vous recommandons d'utiliser si vous avez le projet de mener une veille constante et rapprochée tout au long de l'année.

Vous devez utiliser des contacts locaux. Vous en trouverez de deux sortes. Soit, vous pouvez faire appel à une société locale de mystery shopping, soit à un détective privé (local aussi). Ces deux professions se retrouvent facilement sur le net ou dans les annuaires nationaux. Ce système vous permet de suivre vos concurrents à la trace, n'importe où dans le monde, pour un budget abordable.

Ces potentiels prestataires ne vous connaissent pas et réciproquement. Ils vous demanderont soit la totalité du budget, soit une provision. Vous ne pourrez pas y échapper. Si vous faites appel à de petits business, ce sera bon marché et toutes les surprises sont envisageables. Si vous faites appel à une grosse structure, il n'y aura aucune surprise, ni bonne ni mauvaise, mais la note sera salée.

S'il vous faut un profil particulier pour cette visite sur un salon étranger… Vous avez à portée de doigts le plus grand réseau mondial de correspondants à l'étranger. Je vous explique l'astuce.

S’inscrire sur un site international de rencontres (Meetic). Puis, faire une recherche de profils sur la zone en question. Ça vous prendra dix minutes pour comprendre comment ça marche. Ce qui est chouette, c’est que vous pouvez facilement modifier vos paramètres. Par exemple, si vous cherchez quelqu’un habitant dans la région de Stockholm, vous pouvez changer votre profil en vous enregistrant dans la ville de Stockholm. Ensuite, vous demandez à voir tous les profils qui habitent dans un rayon de X kilomètres. Vous créez votre profil en précisant que vous êtes à la recherche indifféremment d’un homme ou d’une femme. Le nombre de profils sera faramineux, alors vous pouvez vous permettre le luxe de demander ceux qui parlent français ou ceux qui ont un bac+5 si vous voulez. Ensuite, vous envoyez une proposition sous forme de message à tous les profils sélectionnés en faisant des copiés collés. La méthode est assez exotique et je l’ai utilisée avec succès. Vous tomberez sur des gens qui s’ennuient un peu. S’ils sont sur un site de rencontre, c’est qu’ils s’ennuient quand même un minimum. Le luxe est de trouver des gens qui parlent français, qui aiment ça et qui ont quelques heures à perdre.

www.meetic.fr

Vous pouvez tenter le même coup sur Facebook, mais ça marchera beaucoup moins bien car comme vous n’êtes pas dans les contacts des gens ciblés, vos messages risquent de ne pas être lus. De plus, vous ne pouvez pas faire de sélection avec comme critère la langue parlée, sauf si vous allez sur un groupe d’expats francophones, ce qui peut être une très bonne idée.

N'essayez surtout pas ça avec Tinder. Sur Tinder, vous devez cliquer sur les profils qui vous intéressent. Et si ce profil est intéressé par vous, alors c'est un match. Sauf avoir un profil de super beau gosse, vous risquez d'attendre longtemps avant de trouver quelqu'un prêt à vous donner un coup de main pour la visite de votre salon.

Moi, je ne sais pas pourquoi, j'ai gardé toute mon affection pour les sites de rencontres. Où vous savez que les gens sont en demande de quelque chose, même si ce n'est pas de jouer à l'espion pour vous.

N'oubliez pas de demander à cette personne d'enregistrer tout ce qu'elle fait durant le salon.

9. La corruption

Vous voulez de l'info bien chaude ? Achetez là !

Voilà, c'est clair, direct et sans ambiguïté. Vous pouvez le faire en soudoyant deux types de cibles :

- les fonctionnaires des Finances
- les employés ou ex employés de la cible

On en parle régulièrement dans la presse ou à la télévision, surtout avec d'anciens cadres et je déteste cette méthode, encore une fois parce qu'elle est trop risquée.

S'il est probable que tout le monde soit corruptible à partir d'un certain prix, l'expérience montre que celui qui trahit correspond à l'un ou l'autre de ces critères :

• a besoin de beaucoup d'argent pour payer alcool, drogue, dettes, maladie ou putes (ce qui peut être cumulatif).

• homme, intelligent, a dépassé 40 ans, n'a pas atteint ce qu'il croit mériter dans sa carrière.

• a développé une rancœur tenace contre son organisation (ce qui justifie sa future trahison).

• contrairement à certains traîtres dans le domaine du renseignement d'Etat, vous n'en trouverez aucun qui le fera par conviction. Cependant, il y en a qui le font simplement pour se sortir d'un colossal ennui.

Recruter une taupe est un travail long et fastidieux. Sauf si vous en connaissez une potentielle dans votre environnement immédiat.

Sachez que si vous demandez à quelqu'un « un petit service », le pire qu'il puisse se passer, c'est que ce quelqu'un refuse. Et quand cette personne refusera, elle le fera par peur de se faire prendre, pas très souvent par éthique. Je vois mal cette personne déposant plainte pour tentative de corruption de fonctionnaire.

Ce livre est écrit pour que des managers l'utilisent. J'ai voulu en faire un outil de travail. Si vous devez commencer à passer vos après-midis dans le café préféré des fonctionnaires des Finances, dans l'espoir de nouer un contact, je suis certain que vous y parviendrez. Et il est tout aussi possible que ce contact finisse par vous rapporter ce que vous en attendez. Mais ce n'est pas un job de cadre. Trop long. Trop cher. Trop aléatoire. Terriblement illégal.

Je passe.

10.Surveiller les brevets de la concurrence

Un brevet est un titre de propriété industrielle qui confère à son titulaire un droit exclusif d'exploitation sur l'invention brevetée. Ce titre a une durée limitée, généralement 20 ans, voire 25 dans le cas de certains produits pharmaceutiques. Le brevet n'est valable que sur un territoire déterminé. Le contenu d'un brevet reste secret entre la date de dépôt de la demande et la date de publication. Dix-huit mois après la date de dépôt, le dossier de brevet est publié intégralement.

Le chapitre sur l'analyse concurrentielle a une visée essentiellement marketing ou commerciale. La veille technologique, ou juridique n'est pas un autre métier, seulement une autre spécialisation, qui n'est pas la mienne. J'ai été consultant suffisamment longtemps que pour ne pas répugner à parler d'un sujet dont j'ignore tout, mais c'est quand même autre chose de l'écrire et pire encore de le diffuser moyennant finance.

Checker les brevets de vos concurrents ne m'intéresse ici que dans ce cadre. Où en est votre concurrent, que fait-il, ou va-t-il, êtes-vous largué ou en avance ? Rien d'autre.

J'ai longtemps travaillé pour un bureau d'avocats spécialisé dans les droits de propriété. Mes missions consistaient à retrouver les ayants droit d'un brevet. Parfois, le brevet était déposé depuis longtemps et…expiré. J'avoue avoir été plusieurs fois tenté de ne pas retrouver le bénéficiaire légal et de profiter du non-renouvellement du brevet. Je ne l'ai jamais fait car je suis un bon garçon.

Vous verrez avec horreur que la plupart des textes de ce chapitre sont de vulgaires copiés collés. N'hésitez pas à

m’envoyer des pierres virtuelles. Pour ma défense, des fois que j’aurais comme un début d’envie de l’assurer, je présente ici des sites de recherche de brevets et chaque site a sa présentation résumée. Je l’ai à chaque fois reprise car je ne voyais pas l’intérêt de réinventer le fil à couper le beurre.

Il existe quelques moteurs de recherche spécialisés.

Pour la Belgique

https://bpp.economie.fgov.be/fo-eregister-view/search

Cet outil vous permet de consulter les brevets complets du Registre belge des Brevets, ainsi que les données bibliographiques et même la correspondance entre l’Office de la Propriété Intellectuelle (OPRI) et les titulaires de brevet.

Il rassemble des données concernant la description scientifique ou technologique de nouveaux procédés ou produits technologiques ou concernant les certificats complémentaires de protection belges pour les médicaments et les produits phytopharmaceutiques. Vous pouvez aussi vérifier s’il y a eu un enregistrement préalable de brevets similaires ou apparentés, publiés en Belgique.

La consultation est gratuite et aucune inscription n’est nécessaire (source : economie.fgov.be).

Pour la Suisse

https://www.swissreg.ch/srclient/faces/jsp/start.jsp

Pour la France

https://www.data.gouv.fr/fr/organizations/institut-national-de-la-propriete-industrielle-inpi/

Au niveau européen

https://www.epo.org

Grâce à sa couverture mondiale et à ses fonctions de recherche, Espacenet offre un accès gratuit aux informations relatives aux inventions et aux développements techniques de 1782 à nos jours.

Espacenet est accessible aux débutants comme aux experts et est mis à jour quotidiennement. Il contient des données de plus de 120 millions de documents et brevets du monde entier. Des informations complémentaires permettent de déterminer si un brevet a été délivré et s'il est encore en vigueur.

Vous pouvez utiliser Espacenet pour :

- Chercher et trouver des publications de brevets
- Faire traduire automatiquement des documents et brevets
- Suivre les progrès de technologies émergentes
- Trouver des solutions à des problèmes techniques
- Découvrir ce que vos concurrents mettent au point.

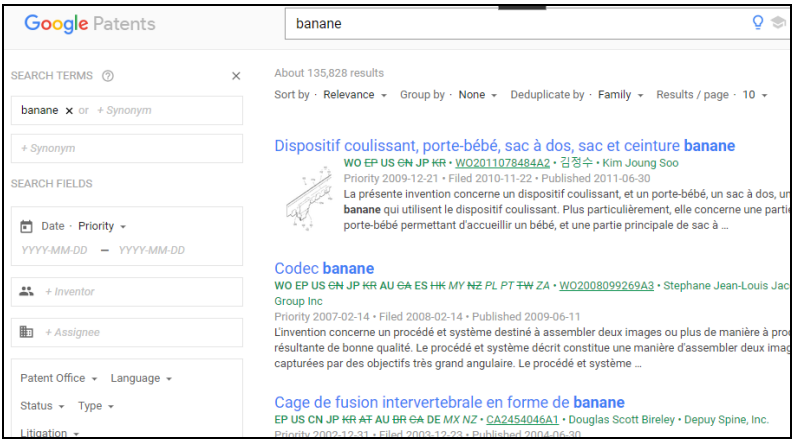
(Source Espacenet)

Au niveau mondial

https://patents.google.com/

Comme souvent, Google n'aime pas être en reste. Google Patents, c'est le Google que l'on connait, mais pour la planète des brevets.

Ce n'est pas qu'une simple compilation des brevets mondiaux, c'est un vrai moteur de recherche qui fonctionne comme le Google que nous utilisons chaque jour. Cerise sur le gâteau, les brevets sont traduits en anglais.



PATENTSCOPE

La base de données PATENTSCOPE permet d'accéder aux demandes internationales selon le Traité de coopération en matière de brevets, en texte intégral le jour même de leur

publication, ainsi qu'aux documents de brevet des offices de brevets nationaux ou régionaux participants.

Les recherches peuvent être effectuées par mots clés, par noms de déposants, par catégories de la classification internationale des brevets et au moyen de nombreux autres critères de recherche dans différentes langues.

https://www.wipo.int/patentscope/fr/index.html

Sachez qu'il est possible aussi de recevoir des alertes, par exemple tous les nouveaux brevets d'une société en particulier ou le suivi d'une technologie.

11.Tracer les modifications d'un site

Certains outils en ligne vous permettent de garder trace de modifications apportées à un site web. Ils sont particulièrement utiles lorsqu'on désire faire le suivi d'un site en particulier. Celui de votre concurrent bien sûr. Mais aussi celui de votre nouveau partenaire. Connaître les modifications du site d'un partenaire commercial, c'est aussi comprendre ce qui le motive à travailler avec vous aujourd'hui.

La version gratuite de cet outil vous permet de suivre 5 sites web. Il vous indiquera quels ont été les changements apportés à ces sites depuis votre dernière visite. En cliquant sur l'hyperlien de ces sites, vous verrez à l'écran les textes qui ont été modifiés ou ajoutés, surlignés de couleurs particulières. Vous aurez également l'option de recevoir par mail, à la fréquence désirée, une alerte vous indiquant ces

changements. Un abonnement payant existe, qui vous permet de traquer plus de sites.

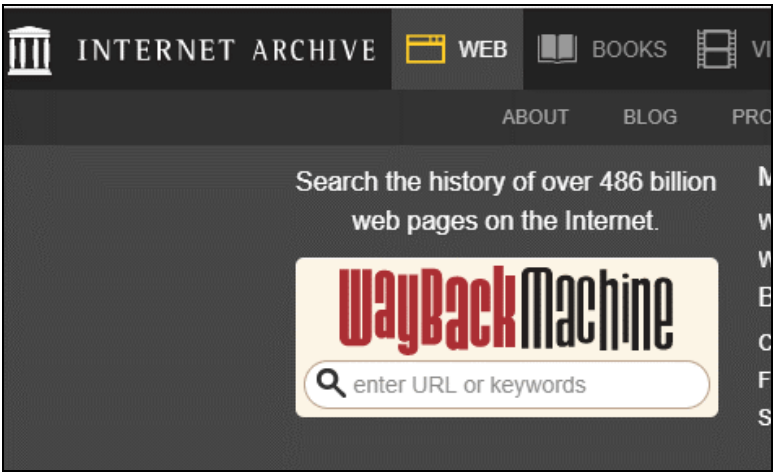
http://www.trackengine.com

L'outil gratuit de veille par excellence. Vous pouvez aussi voir les changements de prix d'un produit ou les modifications de stock sur un site…Gratuit et pas compliqué (si vous vous débrouillez en anglais). Ici, nous surveillons l'avenir d'un site. Mais il est tout aussi intéressant d'étudier son passé, ce qui permet de checker l'évolution d'une entreprise.

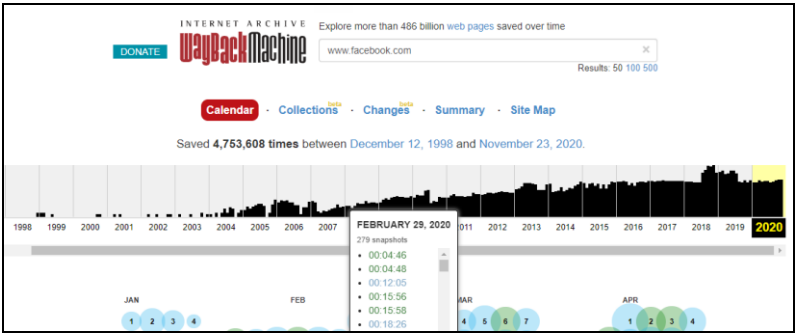
Savez-vous que l'intégralité du web est archivée ? En effet il existe un site où vous pouvez trouver l'historique de la plupart des sites internet. Très intéressant pour voir l'évolution de votre concurrence ou de votre nouveau distributeur.

http://www.archive.org

Quand vous arrivez sur le site, ça se présente comme une grande bibliothèque gratuite. Pas de panique. En haut à gauche de l'écran, cliquez sur l'icône « web »



Ensuite le moteur de recherche « waybackmachine » apparait. Vous tapez l'url de la société que vous voulez suivre, ici en l'occurrence www.facebook.com



L'image vous propose un graphique évolutif avec la date du premier changement opéré sur le site, jusqu'au dernier changement opéré.

Plus bas, vous avez un calendrier avec des dates surlignées. Quand vous cliquez dessus, vous recevez une image du site à cette date précise.

12.S'abonner à la newsletter de votre concurrent

Beaucoup d'entreprises proposent à leurs clients et prospects de s'abonner à leur newsletter. On y apprend des tas de choses comme :

• Comment sont traités les gens qui s'inscrivent ?

• Comment répondent-ils aux emails ?

• L'information qu'ils fournissent est-elle valable ?

• Que font-ils d'original que vous ne faites pas ?

• Leurs nouveautés.

• Les nouveaux collaborateurs parfois.

• Les collaborations avec de nouveaux partenaires.

• Photos d'installations, de produits, de collaborateurs.

C'est facile, ça prend deux minutes et ça peut être intéressant. Par prudence, vous prendrez soin de ne pas faire envoyer la newsletter sur votre adresse professionnelle mais sur une adresse publique du genre Hotmail, Yahoo, Gmail (notez quand même que certaines newsletters ne sont accessibles qu'à partir d'une adresse email étant identifiée comme provenant d'une entreprise).

On s’en doute, ça n’est pas avec cette méthode que vous allez découvrir un extraordinaire secret chez votre concurrent. Mais souvent, c’est ça le renseignement. Ce que vous ne voyez jamais au cinéma sinon vous quitteriez la salle, mort d’ennui. Nous sommes souvent dans un travail de fourmis, qui demande patience et persévérance.

13.Tout savoir de la stratégie en ligne de votre concurrent

Le marketing digital est une branche du marketing qui me passionne. Je sais que ça me donne des airs de geek et je l’assume très bien. Cependant, ce chapitre n’est pas consacré au marketing digital. Mon job ici ne consiste pas à vous aider à faire la promotion de vos produits ou services mais à vous proposer des techniques de collecte de données.

Nous allons voir différents outils issus du marketing digital, mais dans un esprit de recherche d’information sur une cible, en l’occurrence votre concurrent.

L'espionnage des stratégies marketing des concurrents n'est pas aussi péjoratif qu'il n'y paraît à première vue. C'est simplement un moyen de garder un œil sur leurs stratégies de marketing numérique, leur contenu, leurs mots clés, etc. Et vous le faites pour comprendre pourquoi ils vous dépassent dans certains domaines, ce qui leur permet d'obtenir des résultats et, dans certains cas, c'est même une façon de découvrir ce que vous faites de mieux que vos concurrents - pour continuer à vous améliorer.

Ce n'est pas pour rien que l'analyse de la concurrence est un élément important de l'élaboration d'une stratégie de marketing. En outre, elle vous offre une excellente occasion de faire des analyses comparatives pour comprendre dans quelle mesure vos efforts de marketing portent leurs fruits.

Et la vérité est que vos concurrents vous espionnent probablement aussi. Si vous êtes mieux classé dans les moteurs de recherche, ils voudront savoir ce qu'ils peuvent faire pour changer cela. Si vous êtes plus engagé sur les médias sociaux, ils voudront savoir comment améliorer leur stratégie de médias sociaux afin d'obtenir des résultats identiques, voire meilleurs. Si le blog de votre entreprise fait des vagues dans votre créneau, ils voudront améliorer leur propre contenu pour pouvoir surpasser le vôtre.

L’analyse des mots clés du concurrent

Les mots-clés sont incontournables si vous souhaitez être bien référencé. Ils boostent votre visibilité, améliorent le trafic sur votre site et parfois, ils permettent d’attirer une audience qualifiée et d’améliorer le taux de conversion.

Avec SEMRush, vous pouvez facilement rechercher n’importe quel domaine, mot-clé ou URL et effectuer une recherche concurrentielle détaillée. Vous serez en mesure de voir ce que font vos concurrents, quelles sont leurs stratégies publicitaires, quels types de liens ils obtiennent et plus encore. Vous pouvez également utiliser les données fournies pour comparer les domaines entre eux. Pour autant, si vous désirez seulement obtenir les mots-clés de vos concurrents, insérez les URL des sites de vos rivaux et vous

obtiendrez une liste de ces derniers avec le nombre de visites que chacun a réussi à générer.

Vous obtiendrez aussi la page de résultats sur laquelle apparaît le site de votre concurrent pour les différents mots-clés. Vous pouvez tester gratuitement SEMRush pendant une semaine puis il vous en coutera 99 dollars par mois.

https://www.semrush.com/

Si vous voulez connaître l'historique publicitaire de votre concurrent le plus proche ET des données montrant ce qui a fonctionné et ce qui n'a pas fonctionné pour lui, SPYFU est un superbe outil.

En ajoutant cet outil à votre kit, vous serez en mesure de rechercher n'importe quel domaine et de découvrir tous les endroits où le domaine apparaît sur Google. Comme indiqué sur le site de Spyfu, vous pourrez ainsi voir "chaque mot-clé acheté sur AdWords, chaque classement organique et chaque variation d'annonce sur une période donnée".

Spyfu est particulièrement utile pour la recherche de mots-clés. Lorsque vous utilisez Spyfu, il vous suffit de saisir le domaine de votre client et de le comparer à celui de vos concurrents.

Quelques fonctionnalités, mais il y en a vraiment beaucoup :

- Outil d’espionnage des mots clés des concurrents sur AdWords

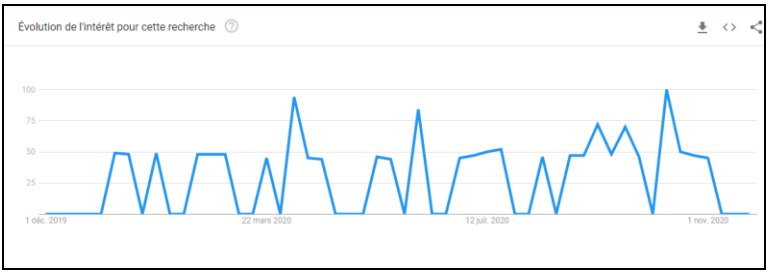
- Trouvez les mots clés des concurrents que vous n'achetez pas déjà
- Historique du classement des mots clés SEO
- Découvrir et étudier l'ensemble du comportement de vos concurrents en ce qui concerne leur marketing digital

Elément non négligeable, la prise en main est rapide, simple et intuitive. Préparez-vous à être soufflé. En bref, vous deviendrez le meilleur espion du marketing numérique de l'industrie.

Vous pouvez utiliser gratuitement Spyfu, mais vous n'aurez pas accès à l'ensemble des informations. Si l'étude du marketing digital des entreprises est tout ou partie de votre activité, un investissement de 39 dollars par mois ne sera pas abusif.

https://www.spyfu.com/

Google Trends est un outil gratuit de mesure de requêtes. Il ne fait pas que ça, mais je ne l'utilise que pour ça. Il me permet de savoir sur une période donnée, quelle est la fréquence des recherches sur Google pour un terme ou une expression donnée, le nom de votre concurrent par exemple.



https://trends.google.com/ est gratuit

Le marketing de votre concurrent sur Facebook et Instagram

Facebook lui-même encourage et permet à quiconque de consulter les publicités que les entreprises et les organisations diffusent sur le site. En mars 2019, Facebook a lancé un outil appelé Ad Library, destiné à promouvoir la transparence sur la plateforme. Ad Library permet à quiconque de rechercher et de consulter toutes les annonces actuellement en cours sur le site, y compris les annonces Instagram.

Il existe d'autres méthodes et outils qui peuvent être utilisés pour évaluer et analyser les publicités Facebook des concurrents, mais j'ai constaté que la bibliothèque de publicités Facebook est l'option la plus facile et la plus fiable qui soit. C'est un outil simple et assez robuste qui peut être utilisé pour en apprendre beaucoup sur ce que font vos concurrents.

Filtrer par impressions

L'une des meilleures caractéristiques de la bibliothèque d'annonces est la possibilité de filtrer les annonces en fonction des impressions. Facebook définit une impression comme le nombre de fois qu'une publicité apparaît à l'écran pour la première fois. Si vous êtes en concurrence avec de grands noms, il y a de fortes chances qu'ils diffusent un grand nombre de publicités différentes. Le filtrage par impressions est un moyen facile de déterminer celles qui sont montrées et vues par le plus grand nombre de personnes.

Pour filtrer les impressions, commencez par entrer le nom de l'organisation ou de l'entreprise que vous souhaitez consulter dans la barre de recherche et sélectionnez la page Facebook lorsqu'elle s'affiche. Ensuite, sélectionnez Filtrer par impressions, puis triez par ordre croissant ou décroissant. La liste des publicités actives s'affichera alors en fonction des filtres que vous avez activés.

Vous pouvez également utiliser la bibliothèque de publicités Facebook pour déterminer les types de médias que vos concurrents incorporent dans leurs publicités. Lorsque vous créez des publicités Facebook, vous pouvez choisir parmi un certain nombre de formats différents, notamment des photos, des vidéos, des histoires, des diaporamas…

Il vous suffit de dresser une liste de vos principaux concurrents, de rechercher leurs annonces dans la bibliothèque et de noter les formats ou types de médias qu'ils utilisent. Facebook vous indiquera même si une annonce comporte plusieurs versions et vous montrera ce

qui est différent pour chacune d'entre elles. Dans la plupart des cas, ce sont différents médias ou messages qui sont testés afin de déterminer lequel est le plus performant lorsqu'il est diffusé.

Les messages sont un autre bon élément des publicités auquel il faut prêter attention, surtout lorsqu'il s'agit d'évaluer les concurrents. Lorsque vous regardez les publicités de vos concurrents sur Facebook, vous devez prêter attention aux titres qu'ils utilisent, aux accessoires de valeur sur lesquels ils se concentrent, aux points qu'ils abordent et à l'appel à l'action qu'ils utilisent. Vous voulez bien comprendre comment vos concurrents se positionnent, ainsi que leurs produits, et quelles promesses, le cas échéant, ils font aux personnes qu'ils essaient d'atteindre.

Un autre moyen d'obtenir un meilleur pouls des publicités des concurrents les plus performantes sur Facebook est de filtrer par durée. Lorsque vous utilisez la bibliothèque d'annonces, vous pouvez filtrer et remonter jusqu'à 90 jours en arrière pour voir quelles sont les annonces qui ont duré le plus longtemps. Si vous voyez des publicités qui sont toujours actives mais qui ont été lancées il y a plus de 30 jours, cela indique probablement que ces publicités ont été performantes pour vos concurrents.

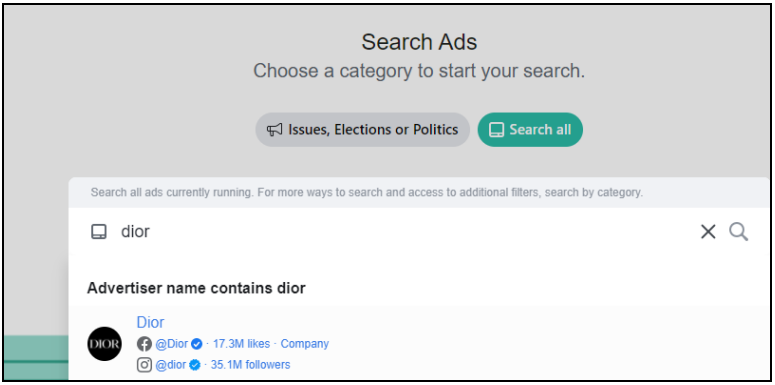
Pour avoir une meilleure idée de la durée de diffusion des publicités, passez du filtrage par impressions au filtrage par durée. Vous pouvez filtrer pour ne voir que les publicités lancées au cours du dernier jour, des 7 derniers jours, des 30 derniers jours ou des 90 derniers jours.

Si vous constatez des tendances et des annonces similaires chez plusieurs concurrents, il vaut probablement la peine de

faire tourner et de tester une annonce similaire pour votre propre entreprise. Et vous n'êtes pas non plus coincé avec Facebook. Vous pouvez utiliser ce que vous avez appris pour tester les publicités Snapchat, Pinterest Ads ou bien d'autres canaux. Lorsque vous recherchez des thèmes communs ou que vous répétez des tendances sur plusieurs pages, faites attention aux images, aux messages, aux offres et aux appels à l'action. Vous devez également prêter attention aux annonces qui apparaissent pendant les vacances, les saisons ou à des jours spécifiques de l'année qui comptent le plus pour vos clients. Il vous suffit ensuite d'appliquer ce que vous avez appris à votre propre marque pour voir comment elle trouve un écho auprès de votre public.

https://www.facebook.com/ads/library

Vous arrivez sur une barre de recherche tout à fait classique. J'ai décidé de m'intéresser de près à la maison Dior.



Je peux faire un tri par pays, c'est-à-dire m'intéresser au marketing en ligne de Dior dans un seul pays, ou dans

plusieurs, ou même dans tous. Une sélection par dates est prévue aussi.

Je reçois immédiatement l'information selon laquelle Dior a plus de 17.000.000. de likes et 35.000.000. de followers. Rien que ça. Facebook me propose 200 publicités de Dior, actives ou pas, selon différents formats, avec possibilité de trier par date et même par plateforme : Facebook, Instagram, Messenger.

Une autre façon d'aller chercher de l'information est d'aller sur la page de votre cible. Cette fois, afin de rester dans le luxe, j'ai choisi Porsche et vous allez jeter un œil sur « transparence de la page »

Je clique sur « see all ». Pour vous qui êtes couramment unilingue, ce sera « voir tout ». Dans le bas de la page, je peux voir si cette page fait de la publicité pour le moment. Je n'ai plus qu'à cliquer et je reviens, avec les résultats, sur la page de la librairie Facebook.

Analyser le site de vos concurrents

Que vous soyez un informaticien chevronné ou pas n'a aucune importance. Vous DEVEZ étudier les performances de vos concurrents en matière de site. Leurs points faibles seront vos points forts, et leurs points forts seront vos défis.

Si vous souhaitez recueillir des informations sur le site web de votre concurrent, il existe des centaines d'outils gratuits ou payants. Pingdom est l'un des outils de surveillance de sites web les plus populaires. Avec cet outil, vous pouvez simplement saisir une URL et obtenir des tonnes d'informations sur la vitesse de chargement du site. En plus des temps de chargement et de réponse, il offre des détails spécifiques et des suggestions d'actions.

Pingdom propose également une surveillance des utilisateurs réels, qui vous permet de recueillir des données sur les comportements des visiteurs d'un site, d'identifier les tendances et d'améliorer l'expérience des utilisateurs. Par exemple, Pingdom vous permet de savoir par quel biais un visiteur arrive sur un site, ce qui est une information au moins aussi importante que de connaître les faiblesses du site.

Certaines fonctionnalités sont gratuites, vous pouvez avoir 2 semaines d'essai avant de payer 10 dollars par mois.

https://tools.pingdom.com/

14.Les groupes de discussions

Vous suivez un blog parce que vous êtes intéressé par le point de vue d'un auteur en particulier. Alors qu'un groupe de discussion est généralement axé sur un certain sujet, et de nombreuses personnes différentes y publient leurs commentaires et questions sur ce sujet. Vous suivez un groupe de discussion parce que vous vous intéressez à un sujet précis. Un blog est mené par une personne, un groupe de discussions, par ses participants. C'est surtout ce dernier point qui en fait la différence.

Tout comme il existe des moteurs de recherche de blogs, il existe aussi des indexations de newsgroups.

Ces groupes (plusieurs milliers) sont hébergés sur le réseau mondial des serveurs de newsgroups appelé Usenet. Son principal objectif est d'offrir un réseau où les utilisateurs peuvent publier librement des informations, qui sont ensuite diffusées. Cela permet à d'autres personnes d'accéder à l'information facilement et aussi rapidement que possible.

Usenet est considéré comme l'un des plus anciens réseaux. En fait, il a été conçu en 1979. Cela signifie qu'il a été mis en place avant le World Wide Web. Pour accéder aux groupes de discussion Usenet, il vous faut un bon fournisseur Usenet.

Il existe des centaines de milliers de groupes de discussion sur le serveur et il est possible pour tout utilisateur d'en créer un nouveau. Usenet continue d'être un forum mondial illimité de débats et d'échanges d'informations.

Alors que de nouvelles avancées continuent à façonner le monde de l'internet et à remettre en question Usenet en tant que moyen de communication, sa popularité ne cesse de croître. Les gens ont besoin d'une communication non censurée et modérée par les pairs, à une époque où la censure officielle ou plutôt la censure sociale prend le pas sur les libertés d'expression.

Les groupes de discussion peuvent constituer une méthode peu coûteuse pour une petite entreprise qui souhaite en savoir plus sur son secteur d'activité, sur la concurrence et se faire une idée des nouvelles offres de produits. Ces informations peuvent également aider une entreprise à anticiper les tendances du secteur et à surveiller les secteurs connexes.

Les Newsgroups sont très importants dans une recherche de renseignements car :

• Vous recevez l'information des clients de la cible, et souvent sans filtre.

• Vous recevez souvent de l'info émotionnelle sur la perception de la cible.

• Vous avez drôlement intérêt à y aller en faisant une recherche sur vous-même, ça vous permettra de savoir les horreurs que l'on raconte sur vous.

• Vous pouvez y pratiquer l'intox à outrance, pas la peine de vous expliquer comment. Les newsgroups ont inventé la rumeur mondiale en un clic. C'est ici que, grâce à votre dévouement, le monde horrifié apprendra que le nouveau plat préparé fraichement sorti des usines de votre

concurrent, a rendu aveugle la moitié des pensionnaires d'une maison de repos.

Dernier avantage, vous y trouverez parfois des messages rédigés par des employés de la concurrence. Si vous allez sur les groupes et que vous faites une recherche sur la cible, vous y verrez aussi les messages laissés par toute personne possédant une adresse e-mail relative à la boite.

Mauvaise nouvelle, un accès vraiment gratuit à USENET n'existe pas. Enfin si, il en existe. Mais les crises de nerf qui seront la conséquence certaine de leur utilisation vous couteront plus cher que de payer. Dans ce livre, chaque fois qu'un outil est gratuit et de qualité, je le conseille. Et dans nos métiers, il y en a énormément. Mais pas ici. Gratuit signifiera bugs, ralentis, pubs indésirables, et instabilité.

Soyons clairs, beaucoup de gens utilisant Usenet le font parce qu'il n'y a pas ou peu de modération et qu'ils peuvent télécharger du porno sans risque. Mais c'est un très grand outil de renseignement.

Google Groups fait en gros la même chose que Usenet. Gratuitement. Mais Google Groups a exclu un grand nombre de forums pour des raisons diverses, dont la moralité. Ce qui veut dire qu'on n'y trouve pas tout. J'ai abandonné l'utilisation de Google groups car la fonction de recherche des archives Usenet de Google a été interrompue à plusieurs reprises dans le passé, ce qui a rendu difficile la recherche d'un article donné.

Les téléchargements sur les newsgroups ne sont pas traçables via le réseau Usenet.

Usenetserver est payant. Comptez 4 à 8 dollars en fonction des promotions.

https://www.usenetserver.com/

https://groups.google.com/

15.Les blogs

Un blog se distingue d'un groupe de discussion par le fait qu'il est mené par une personne, souvent sur un sujet en particulier. Suivre de près le blog de votre concurrent est un indispensable de votre veille concurrentielle.

L'idée est ici de se faire une idée de l'efficacité de vos concurrents en matière de blogs afin que vous puissiez commencer à élaborer une stratégie qui s'appuie sur leurs succès et exploite leurs faiblesses. Voici quelques éléments sur lesquels vous voudrez vous pencher :

Quels types de contenu de blog vos concurrents publient-ils ? Des didacticiels, des informations sur des produits spécifiques, des vidéos, des articles rédigés maison ou des liens ?

Y a-t-il des lacunes évidentes dans le contenu existant de vos concurrents ? Qualité, originalité, fraicheur de l'info, orthographe…

Beaucoup de blogueurs utilisent un style d'écriture personnel que reconnaît directement le lecteur. Ou, selon le sujet de votre blog, peut-être qu'une approche plus formelle, presque académique, fonctionne mieux. Dans tous les cas,

vérifiez comment vos concurrents traitent cette question. Quand demandent-ils aux lecteurs de faire des commentaires ou des suggestions, et comment formulent-ils ces demandes ? Les lecteurs répondent-ils réellement, et à quels types d'approches ?

À quelle fréquence le blogueur met-il de nouveaux articles sur le blog : la fréquence des publications sur le blog est une question importante. Tous les blogueurs vous diront de publier "fréquemment", sans réellement définir ce que ça veut dire.

Les articles qui reçoivent beaucoup de commentaires et ceux qui n'en reçoivent que très peu : un blog qui reçoit beaucoup de commentaires est un signe que le blogueur est en résonance avec son public. Un blog qui ne reçoit pas ou peu de commentaires laisse probablement les gens indifférents et n'est peut-être tout simplement pas lu.

Certains articles sont mieux accueillis que d'autres, et le succès d'un blogueur repose en partie sur le fait de savoir ce qui fait que ces articles fonctionnent vraiment, afin de pouvoir les répéter. Surveillez les blogs de vos concurrents pour voir quand un article obtient une réponse importante, et regardez quelle est cette réponse.

Les blogs officiels d'entreprises sont moins intéressants que ceux réalisés par des employés ou des clients de la cible. Comme dans les groupes de discussions, vous y trouverez de l'information qualitative, émotionnelle, et parfois sensible : un employé dégoûté par son employeur, l'avis d'un client frustré ou au contraire super satisfait. En gros, le même type d'infos que vous trouverez dans les groupes de discussions.

Si votre cible est un illustre inconnu, pas la peine de trop vous fatiguer : une simple recherche Google vous donnera directement accès aux informations des blogs. Dans le cas où Google vous donnerait des milliers de références, il devient alors intéressant, pareil que pour les newsgroups, de mener une recherche spécifique via un moteur de recherche centré sur les blogs.

http://www.keyblog.fr/ est un moteur de recherche de blogs qui utilise la technologie de Google.

16.Les archives des journaux et revues

Les archives de journaux et revues regorgent d'informations de qualité sur les entreprises et les entrepreneurs. Certaines sont libres d'accès, d'autres sont payantes.

Il est totalement inutile d'aller sur le site d'un média pour y mener vos recherches. Google et la science booléenne sont passés par là. A ce sujet, je vous recommande fortement la lecture approfondie du premier chapitre de ce livre.

Dans l'exemple ci-dessous, je suis à la recherche d'articles parus dans Libération, parlant de détectives privés et donc je tape *site:libération.fr* qui me donnera les résultats uniquement venant de ce journal. Je l'associe à « détective privé » et Google me propose exclusivement des articles parlant de ce sujet dans le journal « Libération ». En cliquant sur « outils » en haut à droite de la page, je vais pouvoir affiner ma recherche en fonction des périodes que je souhaite.

Je précise que c'est en utilisant cette méthode lors d'une enquête sur le possible futur partenaire d'un client, que j'ai trouvé une superbe photo du Monsieur en question, menotté entre deux carabinieri. J'aurais trouvé la photo de toute façon en faisant une classique recherche Google car elle était archivée dans Google Images.

17.Identifier les clients du concurrent

Vous voulez identifier les clients de votre concurrent. Soit parce que vous savez que vous êtes tellement fort que vous allez tous les bouffer. Soit parce qu'ils seront pour vous une source d'informations fantastique.

"J'ai remarqué que vous utilisez la technologie X, avez-vous 15 minutes pour essayer de comparer nos logiciels ? » Dans

une économie de marché libre, il est courant pour les entreprises B2B de débaucher les clients de leurs concurrents.

Une partie de la stratégie commerciale B2B consiste à trouver qui utilise les produits et services de votre concurrent ou qui les complimente. Dans une démarche de prospection à froid par téléphone, avouez que vous marquez déjà un petit point en démarrant la conversation par « je sais que vous utilisez la technologie X ». Normalement, vous allez susciter l'attention.

Un autre avantage de découvrir qui sont les clients du concurrent est le gain de temps. Dans une prospection à froid classique, vous ne savez pas si la personne que vous appelez a besoin ou envie de ce que vous vendez. D'ailleurs, la plupart du temps, la réponse est « non merci ». Mais si vous avez une liste des clients de la concurrence, la question ne se pose plus. Vous savez que le client est utilisateur de ce que vous vendez et vous savez aussi qu'il a les moyens de se le payer. Bonus suprême, puisque vous savez chez qui le prospect se fournit, vous savez forcément annoncer un argument très puissant en votre faveur. Et si vous n'en avez aucun, changez d'entreprise.

Il existe de nombreuses méthodes pour identifier les clients du concurrent. Elles peuvent être simples ou complexes, légales ou pas. Probablement que vous ne pourrez pas les utiliser toutes.

Vérifier sur le site du concurrent. Souvent, vous y trouverez le nom de références clients, mais je n'adore pas trop les références car vous n'aurez que les clients super heureux.

Faites-vous passer pour un client potentiel et demandez des références. C'est bien mais même problème qu'au point précédent. Vous n'aurez que des clients heureux.

Allez faire un tour sur les forums sur Internet en tapant le nom de votre concurrent. Non seulement vous risquez de trouver des noms de clients, mais en plus vous aurez leurs commentaires.

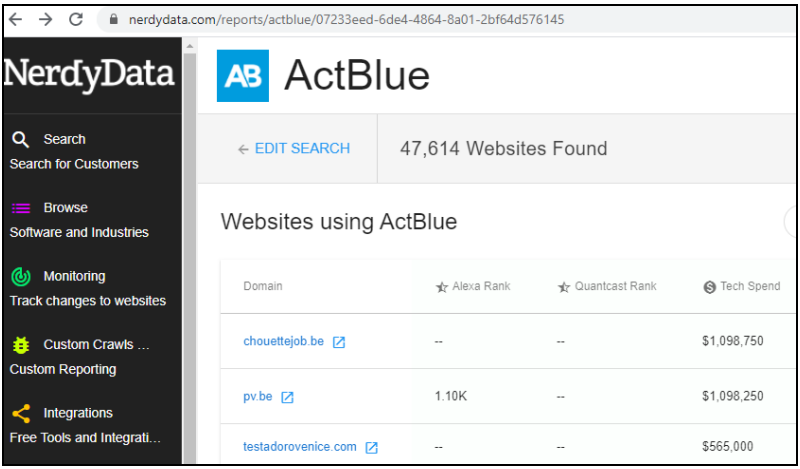
En faisant une recherche Google. Vous tapez le nom du concurrent ou le nom de certains de ses produits si c'est un fabricant, vous arriverez peut-être à dégoter le nom de certains clients.

Vous avez un informateur qui bosse à la TVA et cette charmante personne va vous filer le listing TVA de votre concurrent (c'est très très illégal). Uniquement en Belgique.

Les moteurs de recherche de code source vous permettent de trouver toutes les entreprises qui utilisent une technologie particulière, y compris celle de vos concurrents. Comment cela fonctionne-t-il ? Le moteur parcourt le web à la recherche de codes placés sur des sites web. Les codes peuvent être des CRM, des paniers d'achat, de l'hébergement, du suivi, des analyses, des scripts, des plugins, etc.

Par exemple, si vous vendez une plateforme de paiement en ligne, vous pouvez trouver tous les sites web qui utilisent un produit concurrent.

https://www.nerdydata.com/



Ici, j'apprends grâce à Nerdydata que 47.614 sites utilisent la technologie de ActBlue pour leurs paiements.

Si vous commercialisez une technologie liée au net, ce site est une trouvaille. Non seulement vous pouvez identifier qui utilise quoi, mais vous pouvez aussi savoir qui a changé de technologie et quand.

LinkedIn Sales Navigator permet de filtrer les entreprises qui utilisent une technologie particulière. Il peut s'agir d'un concurrent ou d'un produit complémentaire.

Vous êtes patient ou vous avez de gros moyens et vous prenez en filature les commerciaux ou les camions de livraison de votre concurrent. Bien entendu, cette technique est surtout applicable dans votre pays, même si personne ne vous empêche d'engager quelqu'un pour mener la mission à l'étranger. Soyez attentif à un détail qui peut compter : tout cela est légal. Tant que vous suivez quelqu'un sur la voie publique, personne ne peut rien vous dire, sauf si la personne en question dépose plainte pour harcèlement, ce

qui est peu réaliste. Naturellement, si pour des raisons d'économie et d'efficacité, vous avez collé des trackers sur les véhicules de votre concurrent, ça n'est plus du tout légal.

Il existe une autre méthode, éventuellement complémentaire aux précédentes. Ça coûte un peu d'argent, mais quand on y réfléchit bien, ce sera moins cher que de filer les commerciaux ou les camions de livraison. Faire appel à des étudiants. J'explique. Votre concurrent a forcément une cible. Délimiter la cible. Ici, je vais partir d'un exemple, ce sera plus facile à comprendre.

Imaginons que vous vendiez de l'huile de vidange. La clientèle est composée de garages et de concessionnaires auto. Vous tirez un listing correspondant à la clientèle visée et vos étudiants les appellent tous sous prétexte d'une étude de notoriété. Pour que ça ne coûte pas cher et que ça aille vite, posez un minimum de questions. Ça donne un truc du genre… « Bonjour, c'est Jérôme, je travaille dans un bureau d'études de marché et je réalise une enquête de notoriété. Je voudrais savoir, dans la liste suivante (l'étudiant lit une courte liste de marques d'huile de vidange, comprenant évidemment la marque de votre concurrent, et la vôtre) quelles sont les marques que vous connaissez. Deuxième et dernière question, pouvez-vous me dire dans les marques que vous connaissez, quelles sont celles que vous utilisez dans votre travail ?»

Vous utilisez un étudiant pour deux raisons : la première c'est que ça n'est pas cher. La deuxième, c'est que le taux d'aboutissement des appels est plus élevé. Les gens répondent souvent au téléphone qu'ils n'ont pas le temps de répondre à ces questions. Mais quand vous avez à l'autre

bout du fil, une jeune personne qui miaule « alleeezzz c'est pour payer mes études, y en a pour deux minutes », c'est tout de suite plus compliqué de raccrocher. Je l'ai beaucoup fait quand j'étais étudiant et très rares étaient les personnes qui ne répondaient pas au questionnaire.

Enfin, avantage suprême de la méthode, c'est que vous faites d'une pierre deux coups. Non seulement, vous identifiez les clients de votre principal concurrent, mais vous allez certainement rentabiliser l'opération quand l'étudiant vous remontera quelques prospects bien chauds, pas du tout satisfait des prestations de votre concurrent.

C'est simple, ça va vite et vous aurez créé des listes complètes de clients liés à la concurrence en un ou deux jours. Et ce qui est valable pour l'huile de vidange est valable pour à peu près n'importe quoi. Avec un questionnaire aussi réduit, un opérateur appellera entre 50 et 100 entreprises par jour. Il ne faudra pas très longtemps avant que vous ayez la liste complète, ou peu s'en faut, de tous les clients de votre concurrent.

Sur Facebook ou LinkedIn, vous pouvez savoir qui like une publication ou la page d'une entreprise. Vous pouvez aussi rejoindre un groupe dédié et identifier de nombreux utilisateurs. Ce qui est un peu compliqué ici, c'est que vous devrez faire un tri entre les personnes qui sont proches du produit ou service du concurrent (famille, amis, employés…), et ceux qui en sont les utilisateurs.

18.Identifier les fournisseurs du concurrent

Vous pensez qu'un fournisseur de votre concurrent fait la différence ? Voici quelques outils vous permettant d'identifier le ou les fournisseurs de votre concurrent.

- En tapant le nom de votre concurrent sur GOOGLE, vous aurez peut-être l'heureuse surprise de constater que ce dernier est repris dans la liste des références clients d'un fournisseur.
- Au bluff, ça peut marcher, en vous faisant passer pour un client potentiel, vous exigez de connaître l'origine de certains composants du produit acheté, sous prétexte que chez vous tout doit être bio, iso machin chose ou fabriqué en Europe du nord-est ou n'importe quoi du genre. Un directeur commercial ne vous donnera pas l'information, mais un commercial, c'est très possible.
- Vous pouvez vous mettre en planque à la sortie de chez votre concurrent et prendre en photo tous les camions qui rentrent sur le parking. Vous avez ainsi de bonnes chances de trouver divers fournisseurs. Evidemment, tout ce qui est livré par des sociétés de transport indépendantes vous échappe.
- Si vous recherchez un fournisseur en particulier, il faudra aller au contact, selon toute probabilité. Quand je dis « aller au contact », je ne parle pas d'intrusion. Ni physique (cambriolage) ni informatique (hacking). A mes yeux, l'intrusion est un truc de débile. Même si vous êtes un ex de la CIA, rentrer de nuit dans les bureaux d'une entreprise pour en piller les secrets est un risque énorme. Comme vous ne le ferez pas vous-même, vous en serez à engager

quelqu'un pour le job. Et si ce quelqu'un se fait prendre, vous croyez que le code d'honneur des truands va fonctionner pour vous ? Ou bien qu'il vous balancera en échange d'un avantage ? Encore une fois, la distinction entre cinéma et réalité est de mise. Dans la réalité, le délinquant parle. Sauf s'il craint pour sa peau ou celle de sa famille. Comme vous n'êtes qu'un pauvre cadre sans biceps, il ne vous craindra pas. S'il ne vous escroque pas, c'est déjà un miracle. S'il se fait prendre, vous serez pris.

C'est pareil pour l'intrusion informatique. Aujourd'hui, le délit est tellement coûteux (plusieurs années de prison ferme) que rares sont les gens prêts à prendre le risque. Ceux qui ont des compétences en hacking sont plus faciles à trouver que les spécialistes en cambriolage (n'importe quel consultant en sécurité informatique est un hacker en puissance), mais ils seront aussi bien plus réticents à commettre un sérieux délit qui risque de les envoyer pour fort longtemps au trou. En général, les flics de la CCU (Computer Crime Unit) ne sont pas des imbéciles.

Vous trouverez facilement des propositions de hackers sur le net. La plupart viennent des pays de l'est, mais vous en trouverez aussi venant du Maghreb. Ils vous demanderont une petite avance à payer via Western Union et le job ne sera jamais fait. Et si le job est fait (ça arrive) vous prenez un risque de fou : le hacker vous connaît et il peut vous faire chanter. Et il le fera. Vous l'aurez compris, ce ne sont pas des considérations éthiques qui excluent à mes yeux l'intrusion dans le monde du renseignement économique. Le risque est trop important. Ça laisse des traces.

Donc, j'en reviens à « aller au contact ». Les personnes les mieux placées pour vous fournir l'info sur un fournisseur, ce sont les employés du concurrent. Si vous cherchez un fournisseur en particulier, vous pouvez obtenir l'info…

• En vous faisant passer pour un fournisseur potentiel de ce type de matériel auprès de votre concurrent. Vous tentez de rencontrer l'acheteur de votre concurrent et de le faire parler.

• En vous faisant passer pour un client.

• En invitant un cadre clé à un « entretien de sélection».

• En vous faisant passer pour un journaliste.

• En visitant les locaux du client (en vous faisant passer pour un vendeur de n'importe quoi).

• Sur un salon professionnel en vous faisant passer pour un client.

• En utilisant la même technique « d'études de marché » vue au paragraphe « comment identifier les clients du concurrent », c'est-à-dire en téléphonant à l'acheteur en prétextant une étude sur une gamme de produits, lui citer des marques, demander s'il les connaît et négligemment, à la fin, lui demander avec quelle marque il travaille. Evidemment, ne pas insister s'il ne veut pas répondre.

• Les employés de votre concurrent vont manger à midi. Préparez un bon scénario d'accroche pour entamer une conversation. Une cible intéressante dans ce cas sera le responsable du stock. Vous pouvez bien sûr le rencontrer

par hasard ou essayer sur lui la technique de l'étude de marché.

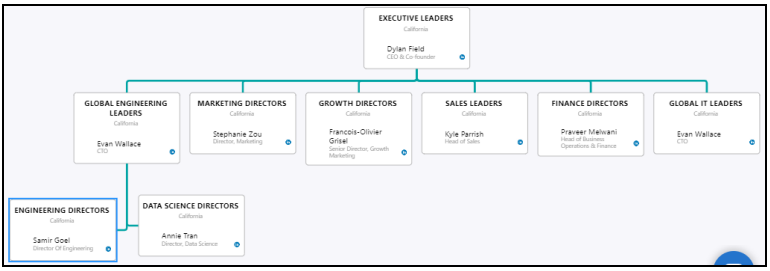
- Utilisez les photos de produits vendus par votre concurrent en les lançant sur les différents moteurs de recherche inversée de photos. Vous avez de bonnes chances d'en trouver l'origine.

19. L'organigramme de votre concurrent en un clic

Identifier les collaborateurs de votre concurrent est relativement facile. Structurer l'information pour obtenir un organigramme de la société, beaucoup moins.

Chartloop est la première plateforme d'organigramme intelligent qui vous permet de visualiser automatiquement la structure organisationnelle de toute entreprise. La plupart des gens utilisent Chartloop pour cartographier leurs comptes cibles de vente, pour construire de meilleures filières de recrutement ou simplement pour obtenir des renseignements stratégiques sur les concurrents.

www.chartloop.com



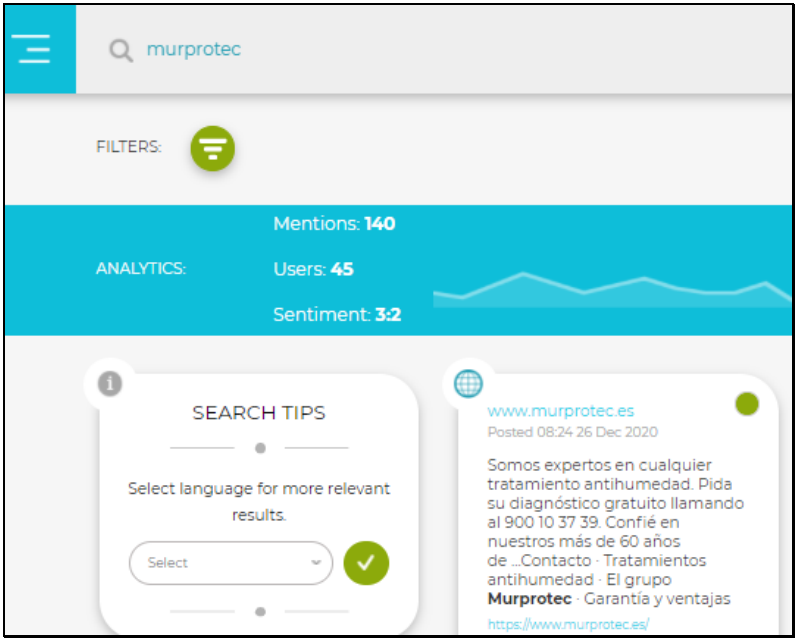
20.La réputation de votre concurrent

Ce que disent les clients de votre concurrent est un atout important. Vous connaissez la perception des forces et faiblesse de l'entreprise. Encore une fois, les méthodes booléennes font parfaitement l'affaire.

Ici, je fais une recherche sur Murprotect, une PME belge prestant des services aux particuliers. Je tape le nom de la société suivi de différents mots entre guillemets : forum, avis, expérience, opinion, review, critique…en incluant « OR » entre chaque mot. Si votre cible est internationale ou anglophone, le nom de la société suivi du mot « review » sera suffisant.

Si vous n'avez pas envie de vous casser la tête, Social searcher fait un excellent travail. Il n'est pas le seul, il en existe beaucoup. Il vous permet de surveiller toutes les mentions sociales publiques dans les réseaux sociaux et sur le web. Vous pouvez mesurer et suivre ce que les gens disent sur votre concurrent, sa marque, ses produits … dans un tableau de bord facile à utiliser et à comprendre. Il y a aussi un système d'alerte qui vous prévient quand un nouveau commentaire est posté sur un réseau.

Outil gratuit dans une certaine limite, assez large. Mais pour 3,5 euros par mois, vous avez accès à tout et c'est impressionnant puisqu'on peut faire une recherche sur les réseaux sociaux avec des mots clés ou des expressions, et aussi de la recherche d'informations sur les personnes ou sur les tendances, au travers de sept réseaux sociaux. On passe à onze réseaux quand une recherche s'effectue sur une marque ou une entreprise.



Le moindre murmure de Twitter ou d'Instagram vous revient aux oreilles en un clic.

Social searcher vous offre aussi des filtres de recherches. Que ce soit la langue, l'expression de sentiments positifs ou négatifs, le réseau social, la date…

https://www.social-searcher.com/

Je suppose qu'il est inutile de vous suggérer de commencer ce type de recherche par vous-même avec cet outil de toute beauté dont la prise en main vous demandera à peu près 8 secondes de concentration intense.

21.Trouver de l'information à forte valeur ajoutée via les banques de données

Nous avons parfois une légère tendance à oublier de faire simple. Il n'y a pas longtemps, un client m'a demandé où il pourrait trouver une base de données d'électriciens. Quand je lui ai répondu « bah, dans les Pages Jaunes », j'ai vu qu'il se sentait un peu bête. Mais il a juste eu un réflexe que nous sommes nombreux à avoir et j'aurais pu avoir le même : chercher compliqué quand on peut faire simple.

Les bases de données publiques sont des mines de renseignements. Nous allons d'abord aborder les bases de données publiques (payantes ou pas) de la Belgique, de la France, de la Suisse et du Luxembourg.

Dans un autre chapitre, j'aborderai les bases de données internationales.

Avant de commencer, une réflexion : beaucoup de ces bases de données apportent une information de grande richesse, gratuite ou à des prix très accessibles. Ne négligez pas une chose très importante, à savoir que ces informations parlent du passé. Parfois d'un passé récent, mais toujours du passé. Obtenir le bilan de votre concurrent ou d'un futur partenaire, c'est fort utile, mais ne négligez pas d'investiguer sur ce qui s'est passé dans cette entreprise depuis que ce bilan a été publié. Nous y reviendrons.

A) La Belgique

La banque Carrefour, qui a remplacé le Registre de Commerce est un outil facile et intuitif, qui s'offre à votre curiosité en 4 langues. La langue par défaut est le

néerlandais, mais vous pouvez facilement changer cela en cliquant en haut à gauche de la page.

http://kbopub.economie.fgov.be

Vous trouvez des informations sur TOUTES les entreprises situées en Belgique, y compris les personnes travaillant sans société mais en personne physique.

Vous pouvez faire des recherches par :

- Numéro d'entreprise
- Par le nom de l'entreprise
- Par activité
- Par autorisation pour une profession en particulier
- Par l'adresse

Ce qui est aussi intéressant, c'est que vous aurez accès aux entreprises actives, mais aussi à celles qui ne le sont plus, ce qui pour un enquêteur est très intéressant.

La première info que vous obtenez, c'est parfois d'apprendre que votre cible est en réalité composée de tas de cibles différentes (évidemment c'est plus rare avec une PME qu'avec une grande compagnie).

Sur cette page, vous n'apprendrez rien d'exceptionnel. Néanmoins, vous trouverez ici :

• La date de création de l'entreprise
• Son numéro de TVA
• Adresse
• Type de société
• Si la société est employeur ONSS
• Le nombre d'unités d'établissement
• si elle est active ou pas
• le nom des administrateurs
• Le nom des curateurs si la société est défaillante
• statut
• type (personne physique ou personne morale)
• date de début
• adresse du siège des personnes morales
• forme légale
• adresse du siège des personnes morales
• données de contact (numéro de téléphone, de fax et adresse e-mail, site internet). Dans la pratique, absentes la plupart du temps
• agréments, autorisations ou licences ayant un intérêt pour des tiers ou soumis à publicité
• radiation d'office à la suite du non-dépôt des comptes annuels

Rien d'éblouissant mais en affinant un peu votre technique, vous serez capable de trouver les filiales d'une entreprise, les liens entre ces entreprises, et les différentes implications d'un administrateur dans différentes sociétés.

Théoriquement, il n'est pas possible ici de savoir si un administrateur est actif dans différentes sociétés. Mais il y a deux façons de contourner l'obstacle, et c'est là qu'intervient le vrai travail d'investigateur. Comme le site permet une recherche par adresse, vous pouvez encoder

l'adresse de la société et voir si d'autres entreprises sont localisées au même endroit.

L'autre façon, c'est en utilisant les noms des administrateurs. Dans les publications du Moniteur Belge (cf. ci-dessous), vous devriez trouver les adresses privées des administrateurs. Vous faites la même chose qu'au point précédent et avec un peu de chance, vous constaterez que de nombreux administrateurs domicilient des entreprises chez eux.

Dans le bas de la page, vous voyez ceci :

Commençons par cliquer sur le Moniteur…

Depuis le 1er juillet 2003, tous les actes des personnes morales ; associations, entreprises, etc… paraissent dans cette annexe du Moniteur belge. Du fait de l'introduction de la Banque-carrefour des Entreprises (BCE), la procédure de publication pour les associations est devenue identique à celle des entreprises. C'est la raison pour laquelle il a été décidé de publier à partir du 1er juillet 2003 les actes des associations avec ceux des entreprises dans une seule annexe. Cette banque de données contient les références des entreprises à partir de 1983 et des associations et fondations depuis le 1er juillet 2003. Il y a des liens vers les images des actes publiés depuis le 01.09.2002 pour les entreprises et depuis le 01.07.2003 pour les associations. Parfois, il existe aussi des liens vers le Moniteur belge même (rubrique Faillites).

1	HILTON INTERNATIONAL CO. (BELGIUM) BVBA GROENPLAATS 32 2000 ANTWERPEN 402.867.427 ONTSLAGEN - BENOEMINGEN 2020-08-31 / 0099969 IMAGE
2	HILTON INTERNATIONAL CO. (BELGIUM) BVBA GROENPLAATS 32 2000 ANTWERPEN 402.867.427 ONTSLAGEN - BENOEMINGEN 2020-03-16 / 0040753 IMAGE
3	HILTON INTERNATIONAL CO (BELGIUM) SPRL GROENPLAATS 32 2000 ANTWERPEN 402.867.427 DEMISSIONS, NOMINATIONS 2019-05-17 / 0067288 IMAGE
	HILTON INTERNATIONAL CO. (BELGIUM) BVBA

Ici, vous avez une trace de toutes les démarches officielles menées par la cible. Vous voyez que dans certaines cases, apparaît le mot « image ». Cliquez dessus et vous aurez le document en question, en format PDF.

Attention que si l'entreprise est située en région néerlandophone, tous les documents seront en néerlandais. Vous ne pourrez pas faire de copié/collé vers un site de traduction car ces documents sont des images.

Vous trouverez ainsi des informations sur :

• Les administrateurs de la cible, ainsi que leur adresse privée
• Les changements d'adresse
• D'éventuelles fusions, scissions, transfert
• Changement d'administrateurs
• Les démissions et les nominations
• Modifications de statut
• Transfert ou vente de certaines branches d'activité
• Augmentation de capital

Le Moniteur belge (en allemand, Belgisches Staatsblatt, en néerlandais Belgisch Staatsblad) est le journal officiel publiant les lois et autres textes réglementaires de l'État belge. Nous avons vu dans le paragraphe précédent que nous pouvions accéder aux modifications légales publiées par la cible. Très simple.

Mais il existe des tas de promulgations publiées au Moniteur Belge qui ne sont pas faites à la demande de la cible. Vous y trouverez arrêtés ministériels, avis, circulaires, décrets, ordonnance, références à un agrément officiel, etc.

Prenons l'exemple avec Hilton.

On commence par taper l'adresse du Moniteur Belge : http://www.ejustice.just.fgov.be/cgi/welcome.pl

Cliquez sur la langue de votre choix et dans la page qui arrive, allez sur « nouvelle recherche » puis introduisez le nom de votre cible dans Mot(s) du texte et « enter ».

On trouve 285 documents relatifs à « Hilton ». Notez qu'ici j'ai demandé les documents dans les trois langues. Ensuite, vous cliquez sur « liste » pour voir apparaître…la liste des documents.

A vous de faire le tri. Car vous allez trouvez de tout, et surtout des choses inutiles à propos d'autres entreprises portant le même nom. Pour lire le document, cliquez sur le bouton comprenant une chaîne numérique à l'extrême droite de la fenêtre. Pas moyen de se tromper.

Ensuite, vous allez faire un petit tour du côté de la Banque Nationale en cliquant sur le bouton « publications comptes annuels BNB » et vous avez accès aux comptes annuels ainsi qu'aux rectificatifs. A l'extrême droite de la page, vous avez un bouton « téléchargement » et vous cliquez dessus pour voir le dernier bilan de votre cible. Tout cela est public et gratuit. Vous pouvez même l'importer sur votre bécane pour le disséquer tranquillement.

Il arrive que des sociétés ne déposent pas leurs comptes annuels. C'est une information en soi, car en général, ce n'est pas bon signe, puisque c'est obligatoire.

B) La France

Pour obtenir des informations comptables sur les SA ou SARL, on peut consulter le site web societe.com ou Infogreffe.fr.

Il faut savoir que ces sociétés sont tenues de déposer dans le mois suivant l'approbation de leurs comptes, au greffe du Tribunal de commerce :

- Le bilan
- Le compte de résultat
- Les annexes
- Les rapports de gestion
- Le rapport général du commissaire aux comptes,
- La résolution de l'assemblée générale des associés (SARL) ou actionnaires (SA) relative à l'affectation des résultats.

Tout intéressé peut obtenir copie de ces documents (qui sont payants chez Infogreffe et société.com).

A titre complémentaire, il est possible d'obtenir un extrait K bis, et le relevé des inscriptions hypothécaires et des nantissements auprès de l'administration de l'enregistrement.

Enfin l'INPI (Institut National de la Propriété Industrielle) est chargé de centraliser tous les comptes de SA et de SARL.

https://www.infogreffe.fr/

https://www.societe.com/

L'AMF est l'autorité des marchés financiers. Vous trouverez beaucoup d'informations sur les sociétés cotées, y compris les sanctions.

http://www.amf-france.org/

L'annuaire officiel des entreprises françaises est tout de même fort riche, mais les résultats dépendent d'une entreprise à l'autre. Vous avez un lien vers les annonces BODACC ou des informations sur les grandes entreprises via le site de l'INPI. Dans certains cas, vous avez et le nom du dirigeant et son adresse privée.

https://annuaire-entreprises.data.gouv.fr/

Le BODACC est le Bulletin officiel des annonces civiles et commerciales. Il s'agit d'un bulletin national qui vient en annexe du Journal officiel de la République Française. Le BODACC assure la publicité de certains actes enregistrés au registre du commerce et des sociétés (RCS), par exemple les avis de ventes et cessions de fonds de commerce, les immatriculations, les créations d'établissement, ou encore

les modifications et radiations de personnes physiques ou morales.

Les informations publiées au BODACC sont issues des registres des greffes des tribunaux de commerce et autres tribunaux civils et commerciaux. Les annonces commerciales sont diffusées sans limitation de durée et sont accessibles à travers le site.

Les informations suivantes sont accessibles via le Bodacc :

- Ventes et cessions de fonds de commerce, projets de fusion
- Création d'établissements, création de fonds, transformation de GAEC
- Immatriculations à la suite de transfert d'établissement principal, de reprise de gérance ou de fusion ou scission
- Procédures relatives aux sauvegardes, redressement et liquidation : jugements, extraits de jugement, ordonnances, avis, règlements et procédures d'insolvabilité
- Modifications des personnes physiques (nom, conjoint, adresse, activité, nom commercial, cessation d'activité…)
- Modifications des personnes morales (capital social, dénomination, nom commercial, activité, mise en gérance, administration, adresse, dissolution…)
- Avis de radiation au RCS des personnes physiques ou morales
- Jugement d'ouverture et de clôture d'une procédure de rétablissement personnel pour insuffisance d'actif

- Avis d'ordonnance conférant force exécutoire à la recommandation de rétablissement personnel sans liquidation judiciaire
- Avis de jugement prononçant un rétablissement personnel sans liquidation judiciaire
- Avis d'arrêt prononçant un rétablissement personnel sans liquidation judiciaire
- Avis de décision de la commission de surendettement des particuliers imposant une mesure de rétablissement personnel sans liquidation judiciaire
- Avis de jugement d'ouverture d'une procédure de rétablissement personnel avec liquidation judiciaire
- Avis d'arrêt d'ouverture d'une procédure de rétablissement personnel avec liquidation judiciaire

Le bodacc offre aussi un service d'alerte.

https://www.bodacc.fr/

L'Institut national de la propriété industrielle propose un moteur de recherche sur les entreprises, qui depuis 2020 offre des données d'identification que l'on trouve partout, mais aussi, d'un même clic, des informations sur les marques, brevets et modèles. L'avantage est que lorsque vous faites une enquête sur une entreprise, vous visualisez aussi ce que cette entreprise a déposé en termes d'innovation.

https://data.inpi.fr/

Vous avez sans doute constaté que je ne m'étale pas trop sur Infogreffe et société.com. Vous pourriez même croire à un chauvinisme belge, une revanche sournoise pour la coupe du monde 2018. Rien de tout ça. La vérité, c'est que l'avenir de ces deux sites est légèrement ébranlé par l'arrivée sur le marché d'un nouvel acteur, Pappers.

Pour faire simple, on va dire qu'avec Pappers, on trouve absolument tout ce qu'on trouve sur les autres sites, à la différence que c'est totalement gratuit. TOUS les documents sont accessibles, y compris les bilans, le chiffre d'affaire, la marge, les comptes, les statuts, l'immatriculation…

J'ai tout de même une petite inquiétude par rapport à ce site. Il ne gagne clairement pas d'argent. Ce qui signifie que d'une façon ou d'une autre, le modèle actuel ne durera pas.

https://www.pappers.fr/

C) La Suisse

La Confédération exerce la haute surveillance et tient un registre central. Celui-ci est actualisé tous les jours, et on y accède par l'index central des registres de commerce, Zefix. Toutefois, la gestion du registre du commerce incombe aux cantons. Ils doivent disposer d'au moins un registre.

Pour l'instant, on compte une trentaine d'offices du registre du commerce en Suisse. Chacun peut y demander des extraits de registre contre paiement d'une taxe et ainsi s'informer sur certaines entreprises. Les extraits peuvent

aussi être consultés sur Internet. Ces informations se trouvent sur le portail Zefix.

Les inscriptions payantes au registre du commerce sont également publiées dans la Feuille officielle suisse du commerce. Les informations essentielles des entreprises enregistrées se trouvent aussi dans l'annuaire suisse du Registre du commerce.

https://www.zefix.ch/

detective [redacted]

Siège:	Châtonnaye
Statut:	active
Adresse:	Chemin du Grand-Rain 1
NPA / Localité:	1553 Châtonnaye
Forme juridique:	Entreprise individuelle
IDE:	CHE-364.454.517
CH-ID:	CH21735690243
OFRC-ID:	1377260
Extrait cantonal:	Web
Office compétent:	Registre du commerce du Canton de Fribourg

But:

exploitation d'une agence de détectives privés sur le plan national et international, spécialisée dans les surveillances, les tribunaux civils et pénaux, contre-expertises, conseils, prévention, client-mystère, audits.

Heureusement, il n’est pas nécessaire de fouiller dans chaque Registre de Commerce cantonal. Mais l’information publique et gratuite est fort limitée. En Suisse, si vous voulez une information complète, il faudra payer. Un site où vous pouvez faire ça prend sans complexe le nom de Moneyhouse.

https://www.moneyhouse.ch

Moneyhouse vous promet les informations suivantes :

- Coordonnées, chiffres clés et direction complète
- Accès aux informations de solvabilité
- Suivre un nombre illimité d'entreprises, personnes et mots-clés
- Découvrir des relations entre les entreprises et personnes dans le réseau
- Recherche détaillée d'entreprises par forme juridique, secteur ou localité

C'est payant, c'est assez cher, mais surtout ça n'est pas top du tout. Quand je veux une enquête de solvabilité, en général les approximations ne m'intéressent pas beaucoup.

Si l'information sur les entreprises suisses est si compliquée à trouver, c'est pour une bonne raison. L'obligation de publication des comptes n'existe pas en Suisse. Relativement peu de bilans sont ainsi disponibles. Pour vérifier une société suisse il convient donc de prendre en compte toutes les informations hors bilan. Et si Moneyhouse a perdu des parts de marchés, c'est aussi parce que des entreprises suisses ont attaqué la société et que divers jugements ont obligé Moneyhouse à refondre sa plateforme.

Vous l'avez compris, si vous voulez de l'information concrète sur des entreprises suisses, il faudra payer et aucune garantie de résultats. Si vous avez les moyens, vous engagerez une agence de détectives spécialisée dans l'information financière.

D) Le grand-duché de Luxembourg

Le Registre de Commerce et des Sociétés (RCS) luxembourgeois constitue un répertoire officiel de toutes les personnes physiques et morales. Ce registre est géré par un groupement d'intérêt économique, le LUXEMBOURG BUSINESS REGISTERS.

https://www.lbr.lu/

Vous y trouverez :

- Numéro RCS
- Date d'immatriculation
- Dénomination
- Forme juridique
- Adresse du siège social
- Liste des documents déposés depuis février 2006

Il y a obligation de dépôt des comptes annuels pour toutes les entreprises, à l'exception de celles qui ont un chiffre d'affaires annuel inférieur à 100.000 euros. Si vous enquêtez sur une petite entreprise luxembourgeoise, ça s'arrête là.
Les grandes entreprises devront fournir plus de détails que les petites. A cet effet, la loi prévoit des schémas complets et abrégés pour le bilan, le compte de résultats et les annexes. Si toutes ces informations sont accessibles pour certaines administrations dans l'exercice de leurs attributions, l'accès pour le grand public ou pour les professionnels est limité aux comptes annuels des sociétés anonymes, des sociétés en commandite par actions, des sociétés à responsabilité limitée et des coopératives. L'accès est gratuit.

E) Accéder aux registres de commerce européens

Grâce au lien suivant, vous allez accéder à l'ensemble des registres des pays de l'union européenne (plus la Norvège, l'Islande et le Liechtenstein). Pour chaque pays, vous avez un descriptif de l'information accessible dans le pays.

Si le lien ci-dessous est trop compliqué à taper, allez sur Google et tapez « répertoire d'entreprises dans les états membres ». Cette petite page n'est rien de moins qu'une source extraordinaire d'informations sur les entreprises.

https://e-justice.europa.eu/content_business_registers_in_member_states-106-fr.do

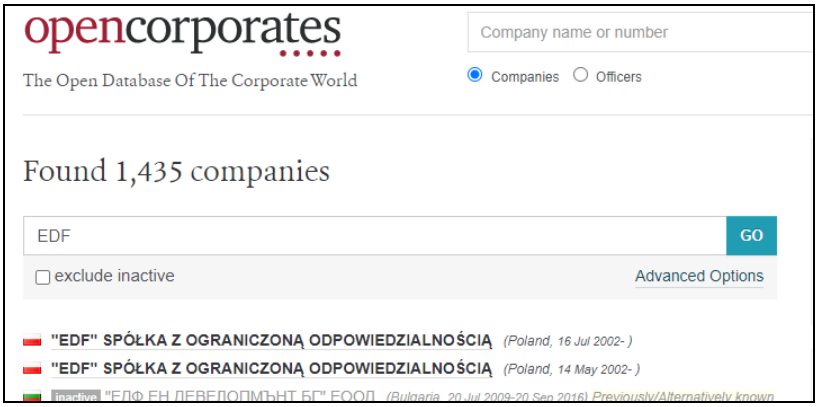
Il existe un moteur de recherche qui fonctionne à travers 20 pays européens, le « european business register ». Il fonctionne à travers diverses sociétés et son accès est payant alors que si vous allez sur l'adresse ci-dessus, c'est gratuit.

Ce moteur payant a quand même un avantage, c'est qu'il vous permet, à partir du nom d'un dirigeant, de le tracer dans l'ensemble des pays membres. Mais tous les pays ne sont pas présents dans ce moteur. Par exemple, la Belgique en est absente.

https://www.ebr.lv/en/company-search

F) Pour aller plus loin…

Opencorporates est une base de données d'entreprises au niveau mondial. L'accès est totalement gratuit. Autant le dire, c'est un outil formidable pour un enquêteur car vous voyez d'un clic la représentation d'une entreprise au niveau mondial.



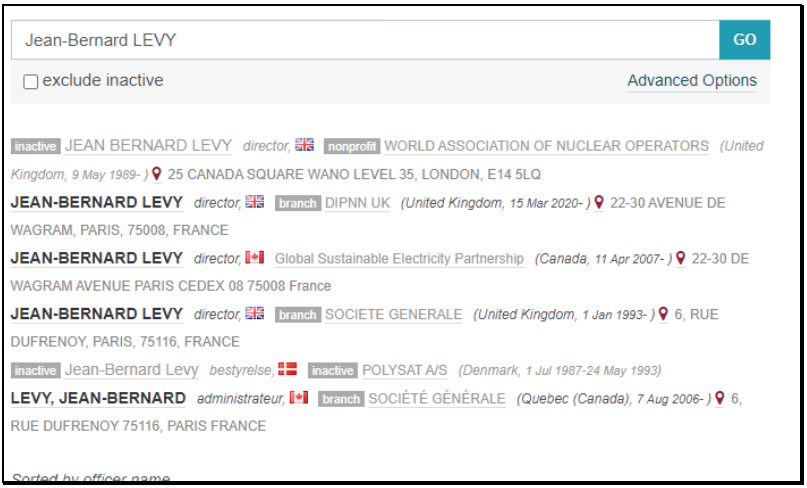
Quand je fais une recherche sur EDF, le site trouve 1435 entreprises à travers le monde. Probablement qu'elles ne sont pas toutes en lien avec un certain fournisseur d'énergie français. A vous de faire le tri. Vous y serez aidé par les options avancées.

Pour un enquêteur, les entreprises inactives sont souvent au moins aussi intéressantes à investiguer que les actives. Opencorporates vous permet de faire une large variété de tris.

Pour chaque entreprise, dans chaque pays, le site vous propose un lien vers le registre de commerce local où vous trouverez entre autres, les documents de création de la compagnie.

Comme vous pouvez faire un tri par pays, vous pourriez apprendre qu'une entreprise a des implantations dans des pays inattendus. Vous trouvez aussi les brevets déposés par une entreprise ou l'une de ses filiales à travers le monde.

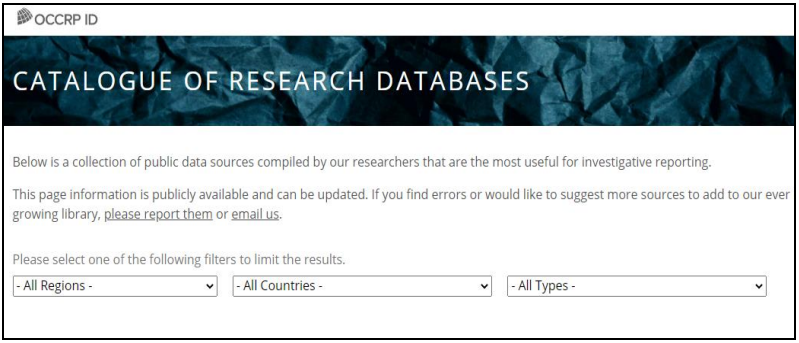
Une forme de tri intéressante est la possibilité de connaître le statut d'une entreprise et de quel type de société il s'agit. Je peux aussi faire des recherches à partir des administrateurs de compagnies. Puisque je suis sur EDF, autant continuer avec Jean-Bernard Levy, son président.



On pourrait croire que le site n'est intéressant que pour les grands dirigeants et les entreprises de gros calibre. Pas du tout. Vous ne trouverez rien sur l'épicerie du coin, mais si vous cherchez de l'information sur une PME, vous trouverez certainement.

https://opencorporates.com/

L'OCCRP (Organized Crime and Corruption Reporting Project) vous sera utile à tracer des personnes, des entreprises et des biens à travers le monde. Il s'agit d'un réseau international de médias et de journalistes indépendants. Vous avez accès à près de 1000 sites d'informations publiques sur les entreprises à travers le monde.



https://id.occrp.org/databases/

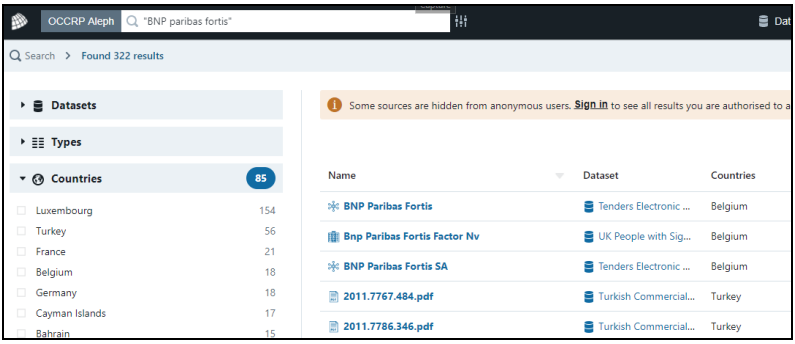
Le projet Aleph fait partie de l'OCCRP. Vous y trouverez des millions de documents du monde entier sur des investigations passées ou en cours sur des individus ou des entreprises.

La plateforme de données Aleph rassemble de vastes archives de bases de données actuelles et historiques, de documents, de fuites et d'enquêtes.

Si le but de ce site est à vocation journalistique afin de dénoncer fraudes et corruptions, il sera aussi utile pour tout investigateur désireux de trouver de l'information sensible. A noter qu'ici, on s'intéresse surtout aux grands. Vous ne

trouverez pas grand-chose sur l'électricien qui a pris votre acompte avant de disparaitre dans la nature.

Mais si on fait une recherche sur un groupe comme BNP Paribas Fortis, on tombe sur des centaines de documents liés à des investigations, dans un grand nombre de pays.



https://aleph.occrp.org/

La base de données de la CIJI contient des informations sur plus de 785 000 entités offshores qui font l'objet des enquêtes des Panama papers, et d'autres scandales financiers. Les données établissent des liens avec des personnes et des entreprises dans plus de 200 pays et territoires. Ici, l'intérêt pour un enquêteur est de l'ordre de la vérification. Vous envisagez un partenariat avec une personne ou une entreprise et vous jetez un œil ici en espérant qu'il ne s'y trouve pas.

Vous n'avez pas envie de travailler avec une entreprise ou une personne qui se trouve sur une liste de fraudeurs ou en liens avec le financement du terrorisme. Malheureusement, ces listes sont dispersées à travers le monde et si vous voulez y mener une recherche, ce sera payant. Altares est le leader mondial de l'information sur les entreprises, en partenariat avec Dun & Bradstreet. Vous y trouverez aussi presque toutes les informations de crédit dont vous avez besoin.

https://www.altares.com/fr/

Deux concurrents :

Le bureau Van Dijk https://www.bvdinfo.com/en-gb/

Ellisphère https://www.ellisphere.com/

En France, vous pouvez accéder à la partie du site de l'Autorité des Marchés Financiers, qui répertorie les acteurs figurant sur les listes noires, ayant fait l'objet d'une mise en garde publiée par l'Autorité des marchés financiers et/ou usurpant un acteur régulé.

https://www.amf-france.org/fr/espace-epargnants/proteger-son-epargne/listes-noires-et-mises-en-garde

Xlek est une base de données unique en son genre. Elle vous donne tout renseignement que vous voulez connaître sur une personne vivant sur le territoire américain : la

recherche de personnes, les registres de propriété (y compris la valeur estimée du bien), les registres de véhicules, les registres des tribunaux (les condamnations sont publiques aux USA), les brevets, l'enregistrement des entreprises, l'enregistrement des noms de domaine et même l'accès au registre des visites à la Maison Blanche. Bien des sites offrent ce genre de prestations. La particularité de Xlek est que l'accès est totalement gratuit et fiable. Deux qualités que vous trouverez rarement aux USA. Les bases de données fiables sont payantes, ce qui n'est pas un problème car les tarifs sont très accessibles. Le problème, c'est que si vous n'êtes pas sur le territoire américain, vous n'y aurez pas accès. Un VPN ne vous sauvera pas car votre carte de crédit sera aimablement refusée.

https://xlek.com/

Il existe aussi des bases de données reprenant le nom des gens soupçonnés de financer le terrorisme ou de façon plus générale, que les banques ne peuvent pas prendre comme client. J'en parle plus loin, dans le chapitre consacré à vos partenaires commerciaux.

VIII. Les meilleurs outils et techniques d'extractions d'Emails

On vous a dit que l'Emailing ne marchait plus, que c'était dépassé, bas de gamme, mal perçu, illégal sans le consentement de la personne qui reçoit votre message, que vous seriez condamné à des amendes ou carrément à la peine de mort. N'importe quoi. A condition d'être prudent et raisonnable, ce qui signifie principalement ne pas harceler les gens. Ma règle a toujours été simple : chaque personne présente dans l'une de mes bases de données peut recevoir un ou deux mails par an. Pas plus. Cela fait plus de dix ans que je pratique et le pire qui me soit arrivé est un courrier d'un ministère me signalant qu'une personne s'était plainte et que j'étais prié de lui envoyer par courrier la confirmation que je n'utiliserais plus jamais cette adresse mail. Dans un total souci de respect de la vie privée, le ministère en question m'a donné l'adresse privée de la personne pour que je puisse lui envoyer ce courrier, ce que j'ai fait.

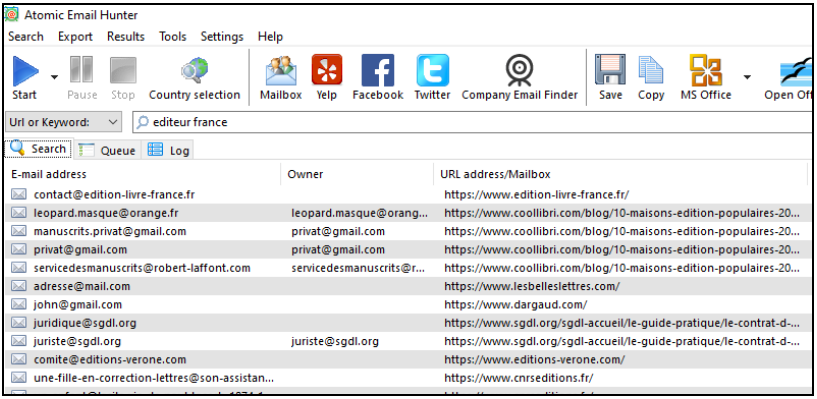
J'ai commencé le grattage d'emails dès la rédaction de mon premier livre. Ma première préoccupation était de trouver un éditeur. Je n'en connaissais aucun à part ceux que je voyais en librairie. Je n'étais ni connu, ni introduit dans les cercles qu'il faut et je savais que seul un livre sur cent est publié. Il n'était pas non plus envisageable que j'imprime le bouquin a des dizaines d'exemplaires pour les mettre un par un, sous enveloppe avant de les envoyer par la poste dans l'espoir d'être repéré par un comité de lecture.

J’ai donc décidé d’utiliser les techniques de scraping de mail. Au départ mon projet n’était pas d’être édité, mais de tout faire moi-même, y compris la promotion du livre via des journalistes. J’ai créé une base de données de journalistes et je m’en suis servi pour faire ma promo. Plus tard, quand j’en ai eu marre de faire le job d’un éditeur, j’ai créé une base de données d’éditeurs francophones et j’ai envoyé des milliers de mails avec la table des matières. Comme j’aime les belles histoires et vous aussi, sachez qu’une vingtaine d’éditeurs m’ont demandé d’envoyer un exemplaire du livre, que six m’ont fait une proposition ferme et que j’ai signé avec l’Express pour le titre « confessions d’un privé ».

Atomic Email Hunter est le premier outil que j’ai utilisé. Il s’agit d’un robot qui va se balader sur le net et extraire des emails de deux façons différentes :

- Vous avez identifié, grâce à Google, des répertoires ou annuaires reprenant les coordonnées d’éditeurs ou de journalistes et vous copiez/collez l’url du site dans Atomic et c’est parti. Si le site n’est pas trop protégé, tous les mails seront avalés par votre petit robot.

- Vous utilisez le moteur d’Atomic avec des critères de recherche par pays ou région. Ça n’est pas d’une folle précision mais ça fonctionne. Il faudra quand même faire un tri manuel pour enlever les adresses qui ne conviennent pas à votre recherche.



Ensuite, je peux extraire les données obtenues et les ouvrir dans un fichier Excel.

Atomic ne fonctionne pas avec les fichiers PDF. Si vous avez un lien vers un fichier de ce type, vous avez quand même la possibilité que ça marche. Vous ouvrez le fichier en cache en cliquant sur le petit triangle inversé puis sur « en cache ».

Enfin, vous copiez l'adresse dans la barre de recherche d'Atomic et vous lancez. L'adresse commencera toujours par « googlecache ».

Vous pouvez l'essayer gratuitement mais ne pourrez pas exporter les données. Vous pourrez donc tester l'efficacité du soft, mais pas profiter des résultats.

Budget 75 Euros

https://www.atompark.com

Un deuxième outil que j'affectionne, c'est Annucapt. Annucapt permet de récupérer les données des principaux annuaires de France, Belgique, Suisse, Luxembourg, Allemagne, Italie, USA, Grande Bretagne, Canada, Espagne, Monaco, Maroc et l'accès aux annuaires mondiaux de Yelp et d'Infobel. L'information est fournie de façon structurée, comme sur un fichier Excel (vers lequel vous pouvez exporter) avec le nom de la société, l'adresse, téléphone, mail, web…

Comme les annuaires vendent leurs données, c'est la guerre permanente entre eux et Annucapt. Très souvent, l'extraction d'un annuaire ne fonctionne plus ou alors partiellement. Annucapt propose très vite une mise à jour qui répare le problème, jusqu'au moment où l'annuaire a de nouveau trouvé une parade…

Globalement ça marche très bien. Annucapt pratique l'extraction classique sur le web, mais ça n'est pas pour ça qu'on l'achète.

Budget 125 euros avec possibilité d'essayer mais vous ne pourrez ni avoir accès à toutes les fonctionnalités ni exporter les données.

https://www.atompark.com/

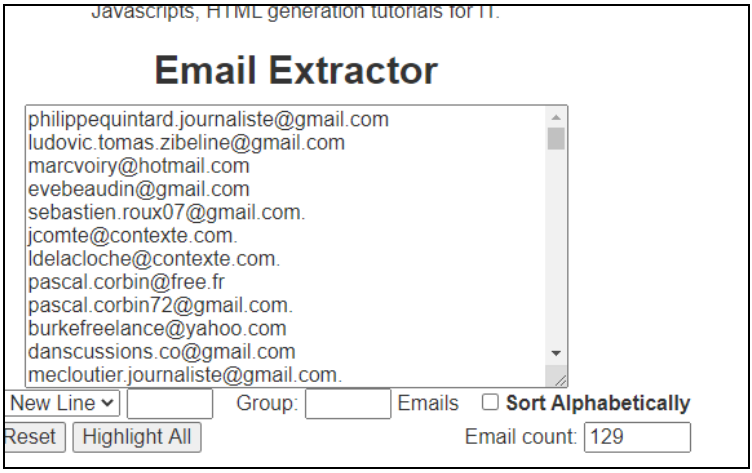
Annucapt n'est pas seul sur son marché mais comme je n'ai jamais utilisé les autres, je n'en parle pas.

Le troisième est un petit outil génial et gratuit qui permet de copier toutes les adresses emails se trouvant sur une page, quel que soit le format du fichier. Vous copiez la page et

vous collez dans Discoveryvip. A droite du mot « separator », vous cliquez sur « new line » et puis sur « extract ».

Un autre point fort de l'outil, c'est que si je fais une recherche google demandant de me trouver des adresses gmail.com de journalistes, je n'ai plus qu'à copier les résultats de Google vers l'extracteur.

Et voilà, je me viens de me créer une base de données de 129 journalistes en quelques secondes. Bien sûr, ça n'est qu'un début.



https://emailx.discoveryvip.com/

J'ai déjà parlé de https://hunter.io/ dans le chapitre consacré au sourcing. Pour rappel, avec cet outil, vous pouvez obtenir de nombreuses adresses email de personnes travaillant dans la même société.

Idem avec https://phonebook.cz/ qui est gratuit dans une grande limite et ramène de nombreux mails à partir de l'URL d'un site.

IX. Espionner sur les réseaux sociaux (socmint)

Le social media intelligence (dont l'abréviation anglaise est SMI ou SOCMINT) fait référence aux outils et aux solutions qui permettent aux entreprises de surveiller les différentes plateformes et conversations sur les médias sociaux, de réagir aux différents signaux reçus sur ces médias sociaux, et de synthétiser ces réactions individuelles pour en déduire des tendances et des analyses fondées sur les besoins des utilisateurs. Vous pouvez bien entendu faire ça pour surveiller votre voisine ou votre ex-mari.

Le social media intelligence permet de rassembler des informations en provenance de ces plateformes de médias sociaux, par des moyens intrusifs ou non. Ceci explique pourquoi on recourt au terme anglais d'« intelligence ». Ici, « intelligence » est ce que votre prof d'anglais appelait un faux-ami. Il n'a strictement rien de commun avec votre niveau intellectuel. Une agence de renseignements se dira « intelligence agency ».

Les sites de médias sociaux offrent de nombreuses possibilités d'investigation en ligne, en raison de la quantité d'informations utiles qui se trouvent au même endroit. Par exemple, vous pouvez obtenir un grand nombre d'informations personnelles sur n'importe quelle personne dans le monde entier en consultant simplement sa page Facebook. Ces informations comprennent souvent les connexions de la personne concernée sur Facebook, ses opinions politiques, sa religion, son origine ethnique, son

pays d'origine, ses images et vidéos personnelles, le nom de son conjoint (ou sa situation de famille), ses adresses de domicile et de travail, les lieux fréquemment visités, ses activités sociales (par exemple, sports, théâtre et restaurants), ses antécédents professionnels, son éducation, les dates d'événements importants et ses interactions sociales. Ces informations sont obtenues de façon directe ou indirecte.

Le renseignement via les médias sociaux est une sous-branche de l'Open Source Intelligence (OSINT). Les données disponibles sur ces sites peuvent être soit publiques soit privées. Je ne vais pas entrer dans le débat de savoir si ces recherches sont légales ou pas. Le débat fait rage chez les chercheurs, principalement américains. Mais on peut dire que si vous collectez sagement ce qui vous est offert, c'est légal. Bien entendu, ce chapitre n'est pas que sagesse.

La facilité d'accès aux informations provenant des réseaux sociaux tient son origine de différents facteurs, principalement humains.

- « Je n'ai rien à cacher » est souvent entendu. Ce qui est assez sot, car si vous n'avez rien à cacher, ça n'est pas pour ça que vous voulez tout montrer.

- L'égo est l'ami de l'espion. Beaucoup de gens, vraiment beaucoup, trouvent qu'il est très intéressant de poster des photos de vacance ou de repas -qui n'intéressent strictement personne- ou encore de partager des articles issus de médias traditionnels ou alternatifs, en se donnant l'impression de défendre une cause ou d'être journaliste. Tout ça pour un « like » de

plus. Comme nous l'avons vu dans le chapitre sur le renseignement d'origine humaine, l'égo est un allié sûr de l'agent de renseignement. Ne vous méprenez pas sur mes propos légèrement teintés de condescendance, l'auteur de ces lignes n'est pas différent des autres humains. Nous avons tous un égo, et c'est une faiblesse facile à exploiter.

- De plus en plus souvent, les propriétaires d'un profil cherchent à masquer une partie de leurs informations. Nous verrons dans ce chapitre qu'il ne s'agit là que d'une illusion de sécurité.

- Enfin, l'aspect technique intervient. Il existe de nombreux outils permettant de collecter les informations sur les réseaux sociaux. S'il n'est pas possible de pirater des sites comme Facebook ou LinkedIn, malgré les promesses de centaines d'escrocs en ligne, il est possible de contourner certaines règles de sécurité.

Types de contenu des médias sociaux

Les gens interagissent sur les réseaux sociaux à différentes fins. Le SOCMINT est intéressé par la collecte de tous les types de contenu, mais la capacité à le faire dépend du niveau de contrôle de la confidentialité défini par chaque utilisateur lors de la publication de messages/mises à jour en ligne. Par exemple, il n'est pas possible de voir les mises à jour d'autres personnes sur Facebook si elles limitent la visibilité d'un post à certains cercles d'amis ou le définissent comme "Seulement moi".

Classifications des plateformes de médias sociaux

De nombreuses personnes utilisent les termes médias sociaux et réseaux sociaux de manière interchangeable pour désigner Facebook, Twitter, LinkedIn et les plateformes sociales connexes. Ce n'est pas absolument faux, mais ce n'est pas tout à fait exact non plus, car leurs fonctionnalités et leurs objectifs sont différents.

Voici les principaux types de médias sociaux classés selon leur fonction :

1. Réseauter et se parler : Cela permet aux gens de se connecter avec d'autres personnes et entreprises en ligne pour partager des informations et des idées. Les exemples incluent Facebook et LinkedIn.

2. Partage de photos : Ces sites web sont dédiés au partage de photos entre utilisateurs en ligne. En voici quelques exemples : Instagram et Flicker.

3. Partage de vidéos : Ces sites web sont consacrés au partage de vidéos, y compris les diffusions vidéo en direct. Le plus populaire est YouTube. Veuillez noter que Facebook et Twitter offrent également un service de diffusion vidéo en direct.

4. Les blogs : Il s'agit d'un type de site web d'information contenant un ensemble de messages liés à un thème ou à un sujet, organisés par ordre décroissant en fonction de la date de publication. Les plateformes de blogs les plus populaires sont WordPress et Blogger, qui est une émanation de Google.

5. Microblog : Il permet aux utilisateurs de publier un court paragraphe de texte (qui peut être associé à une image

ou une vidéo) ou un lien (URL) à partager avec d'autres personnes en ligne. Twitter est l'exemple le plus populaire.

6. Forums : C'est l'un des plus anciens types de médias sociaux. Les utilisateurs échangent des idées et des discussions sous la forme de messages et de réponses affichés. Reddit en est un exemple.

7. Evaluation des produits/services : Ces sites web permettent à leurs utilisateurs de faire le point sur tout produit ou service qu'ils ont utilisé.

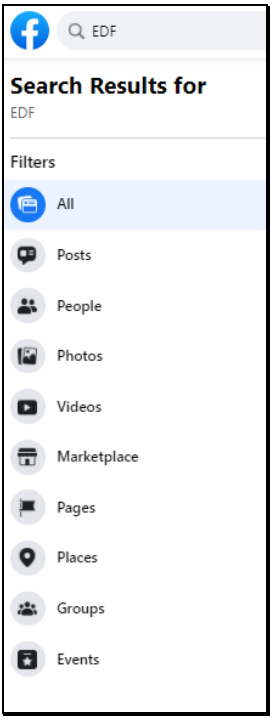
Maintenant que nous avons une bonne compréhension des différents types de médias sociaux, il est temps de commencer à parler de la manière d'utiliser les différents outils et techniques pour acquérir de l'information à partir de ces plateformes.

1. Facebook

Facebook est la plateforme de médias sociaux la plus populaire et compte le plus grand nombre d'utilisateurs au monde. Facebook offrait un moteur de recherche sémantique avancé pour effectuer des recherches dans sa base de données en utilisant des phrases et des mots-clés en anglais naturel. Ce moteur de recherche sémantique appelé Graph Search a été introduit au début de 2013. En 2019, Facebook a supprimé la fonctionnalité de recherche via Graph Search. La puissance de Graph Search représentait un danger réel pour la sécurité de certaines personnes. Mais la nature n’aime pas le vide. Ce formidable outil permettait de faire des requêtes du genre : « femme célibataire âgée

de…à…, habitant telle ou telle ville ». Ça, ça reste encore un peu amusant, mais « homme militaire région parisienne ayant travaillé en Afghanistan », un peu moins. A partir du moment où une technologie a été créée, il est très compliqué de la faire disparaitre. Raison pour laquelle, des outils de remplacement de Graph Search sont apparus. Non seulement ça, mais Facebook a aussi amélioré ses fonctions de recherche.

Imaginons que ma recherche porte sur un sujet passablement sensible comme les centrales nucléaires gérées par EDF.



Je vais recevoir une belle moisson d'informations. Vais-je tomber sur la pépite stratégique qui me permettra de prendre possession de toutes les centrales EDF ? Non, aucune chance. Et si par hasard un distrait ou un maladroit venait à publier une information confidentielle, ça arrive, j'ai vu un soldat annoncer sur sa page une attaque pour le lendemain, le post serait très rapidement effacé. C'est par le croisement des informations que votre mission de renseignement aboutira à un succès.

De façon très simple, je vais ici accéder aux posts publiés à propos des centrales, aux gens qui y travaillent, aux photos et vidéos de centrales, ainsi qu'aux pages et aux groupes dédiés au nucléaire et/ou à EDF, gérés ou pas par EDF. Que ce soit pour les groupes, les gens, les pages, les photos, j'ai encore la possibilité à chaque fois d'affiner la recherche en fonction de différents critères.

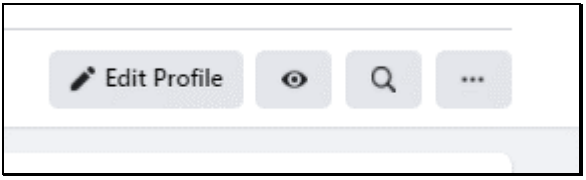
Sur la gauche de l'écran se trouvent les filtres. Vous pouvez les utiliser pour réduire votre liste de résultats et la rendre plus facile à gérer. À la suite de la refonte radicale de Facebook en 2020, les anciens filtres par défaut ne sont plus disponibles. Ils ont été remplacés par une nouvelle liste de 9 filtres. Les nouveaux filtres ont chacun un objectif spécifique et comportent des sous-filtres dédiés qui vous permettent d'affiner vos résultats. Facebook est devenu un moteur de recherche à part entière.

Les nouveaux filtres sont les suivants : messages, personnes, photos, vidéos, marchés, pages, lieux, groupes et événements.

Si vous faites une recherche sur une personne, ça fonctionne même si vous n'êtes pas ami avec elle. Vous pourrez en tout

cas voir des photos prises par la personne elle-même ou d'autres, mais vous ne pourrez pas connaître les évènements auxquels la personne participe, ni si elle est membre de certains groupes, ni le truc important, lire ses posts. Souvent, vous ne pourrez pas voir sa liste d'amis, ce qui est pourtant très important dans une mission de renseignements. Nous verrons plus loin qu'il est quand même possible d'accéder à toutes ces informations soi-disant confidentielles.

Pour lire les posts d'une personne, ceux qu'elle a publiés sur sa page ou sur la page d'autrui, il y a un truc. Ce truc fonctionne partiellement, même si vous n'êtes pas ami avec la personne. Quand vous allez sur la page de la cible, en haut à droite de la page, en dessous de la photo de profil, vous trouvez ça :



Vous cliquez sur la loupe. Si la loupe n'est pas visible, vous cliquez sur « … » et vous verrez la loupe. Vous tapez le nom, le prénom, une combinaison des deux ou un pseudo de la cible. Vous obtiendrez des résultats différents. Des posts invisibles auparavant sont maintenant accessibles. Vous pouvez les trier par années ou par récence.

Il existe de nombreux services en ligne qui simplifient le processus d'acquisition/analyse des informations des comptes Facebook. Souvent, il vous faudra connaître le numéro d'identification Facebook de votre cible.

https://lookup-id.com/ fera ça très rapidement. Attention que le résultat apparait tout en bas de la page, vous pourriez croire que le moteur ne fonctionne pas.

Par exemple, si vous avez besoin de savoir si une personne est membre ou administrateur d'un groupe, une extension pour Chrome permet d'obtenir l'information. Si vous utilisez le navigateur Google Chrome, vous pouvez utiliser l'extension "Multiple Tools for Facebook". Cette extension se concentre principalement sur votre propre profil, mais elle possède une fonctionnalité vraiment intéressante. Assurez-vous que vous avez obtenu le numéro d'identification du profil de votre cible avant de suivre ces étapes. Une fois l'extension installée, allez dans le menu et choisissez "tools" dans le menu de gauche. Vous verrez alors apparaître une barre de recherche dans laquelle vous trouverez le numéro d'identification du profil avec lequel vous êtes connecté. Supprimez ce numéro et remplacez-le par le numéro d'identification de votre cible. Cliquez sur "Rechercher" pour voir les groupes dont votre cible est membre ou administrateur.

L'inconvénient de l'utilisation de cette extension Chrome est qu'il est possible que votre profil soit temporairement banni parce que Facebook le détecte. Cela m'est arrivé plusieurs fois après un usage intensif. Il parait qu'en cas d'utilisation industrielle, votre profil peut être définitivement banni. Soit vous utilisez cette extension avec délicatesse, soit vous avez un faux profil dont vous pouvez vous passer.

Même si cela semble un peu folklorique, Facebook est l'outil de renseignement le plus utilisé. En voici différents usages.

• Check cv. Lors d'une vérification de cv, tout le profil Facebook est passé à la moulinette. Pas la peine d'être trop parano non plus. Si on vous voit en maillot sur la plage ou un peu éméché durant une fiesta entre potes, ça n'est pas ce qui vous fera manquer le job de votre vie. Par contre, et remarquez à quel point c'est fréquent dans votre entourage, des propos complotistes ou xénophobes ne passeront pas. Bien entendu, tout dépend de la virulence de vos écrits. Un ami proche, travaillant pour la ville, a reçu un courrier plutôt acerbe à la suite de l'un de ces posts car « portant atteinte à l'image de … ». Il n'y a pas eu de conséquences graves pour lui ou sa carrière, sinon une certaine rancune à l'égard de ses employeurs.

• Espionnage entre associés. Extrêmement courant. Un associé veut connaître les intentions de l'autre. Ho comme elle est belle la nouvelle maison que vous avez achetée dans le sud de l'Espagne ! Vos vacances aux Maldives. Votre superbe Porsche. Si vous avez l'intention de changer de vie, cela risque de se voir sur Facebook. Pas seulement à cause de votre maladresse, mais aussi à cause des commentaires de vos amis

• Validation de partenaire ou enquête pré-fusion/acquisition. La page du potentiel partenaire est étudiée en profondeur, tout comme celles du dirigeant et des cadres principaux. Tout comme leurs relations.

• Analyse concurrentielle. Idem que le point précédent. Avec en plus, l'usage intensif des outils du marketing digital. Mais ces outils là ne concernent pas les gens, uniquement la compagnie visée et sa politique commerciale et marketing.

• En recherche de personne, c'est l'outil number one. Je ne vous parle pas de recherche de criminels, je n'y connais strictement rien. Mais les gens ordinaires, qui sont recherchés par une famille, ou un notaire, et qui ne se cachent pas. Ou ceux qui ont des dettes impayées, qui ont changé de pays et se croient hors de portée. Une simple photo vous identifiera grâce à une plaque d'immatriculation, la présence d'un bâtiment public ou une simple enseigne de magasin. Vos amis, sans le vouloir ni le savoir, aiguilleront un enquêteur chevronné.

• L'enquête de solvabilité. Lorsqu'il s'agit d'une entreprise, il est relativement aisé de savoir si elle a les moyens de rembourser ses dettes. Lorsque c'est un particulier, les informations publiques sont rares. Avant d'entamer des poursuites, un créancier voudra savoir si le débiteur est solvable. La clé numéro 1 (j'insiste, quand il s'agit d'un particulier), c'est de savoir si le débiteur a un job. Des biens immobiliers. Une voiture personnelle. Et Facebook permet souvent de répondre à ces questions (ou vous donne des pistes pour creuser l'enquête), que ce soit par le profil Facebook, les photos, ou les commentaires des amis (« bravo, bravo, pour ta nouvelle promotion ! »). La plupart des gens qui vous doivent des sous ont un profil sur Facebook.

• Le renseignement militaire. Cela semble absurde de penser que Facebook puisse être un outil de renseignements militaires. Pour un analyste compétent et chevronné, Facebook est une source incroyable d'informations sur une opération en cours. Si je veux obtenir de l'information sur les militaires français déployés au Mali, c'est malheureusement très simple. Je ne vais pas utiliser que

Facebook, mais sur ce site, je vais bénéficier de photos et de vidéos prises par l'armée elle-même, par des journalistes et des soldats. En utilisant des mots clés comme « légion Mali », « opération Barkhane », « militaire français Mali », « légionnaire Mali », le nom de différentes unités qui sont sur le terrain et dont on mentionne le nom un peu partout…je vais trouver des milliers de documents. Chaque document sera assez innocent pris tout seul. C'est l'impressionnante collection de ressources qui me permettra d'identifier : les unités sur le terrain, l'armement, les systèmes de défense, les hommes engagés, avec la possibilité de trouver leur adresse privée. Les photos et vidéos sont commentées. La plupart par des gens qui félicitent ou insultent les militaires mais sans avoir de lien avec le terrain. Ce sont donc des informations sans intérêt. Mais il arrive très souvent que des commentaires viennent des militaires engagés eux-mêmes. Ils donnent des informations qui semblent à priori peu sensibles mais permettent l'identification d'unités engagées et surtout, ils donnent leur nom.

Outils et astuces

a) Créer un faux profil Facebook

Cela vous donne une possibilité de fouiller Facebook à moindre risque et aussi de vous créer une légende si vous voulez devenir ami d'une cible. Pour faire cela, il vaut mieux être intraçable et c'est tout à fait possible.

Au moment de vous inscrire, Facebook vous demandera une adresse e-mail. Rien de plus simple que d'en créer une,

mais le mieux, c'est d'avoir une adresse jetable qui s'autodétruit au bout de quelques minutes.

Quand vous allez sur le site https://10minutemail.com/ , vous recevez une adresse pour une durée de 10 minutes et une boite de réception. Vous vous inscrivez sur Facebook, vous donnez votre adresse jetable, puis vous allez sur votre boite de réception provisoire afin de répondre au mail de confirmation de Facebook, et le tour est joué. 0 trace.

Ensuite, vous allez sur https://thispersondoesnotexist.com/ qui est un site qui génère des photos de personnes qui n'existent pas. Vous relancez le site jusqu'au moment où il vous propose une photo qui vous plait. Quel est l'intérêt ? Le même qu'au point précédent. On ne peut pas tracer la photo avec un logiciel de recherche inversée de photos, puisque cette personne n'existe pas.

A ce stade, vous avez créé un faux profil intraçable.

Ensuite, il faudra vous créer une identité. Tout dépend de l'objectif visé avec votre faux profil. Choisissez votre nom avec soin. Attention, presque chaque personne se créant un faux nom, continue à garder les mêmes initiales. Ajoutez âge, intérêts, date de naissance, job, écoles, en fonction de votre objectif ET en évitant d'être projectif, à savoir créer une fausse identité à partir de la vraie.

Si votre nouveau profil est créé en fonction d'une personne en particulier dont vous voulez devenir l'ami sur Facebook, pensez à créer un profil avec des points communs avec l'univers de cette personne. Nous aimons les gens qui nous ressemblent. Par exemple, vous avez 40% de chance en plus

d'être accepté par une personne si vous avez en commun le nom, ou le prénom, ou la ville, ou l'école, le job…N'en faites pas trop quand même.

Commencez à inviter des amis. Même à notre époque, beaucoup de gens acceptent dans leurs amis Facebook des gens qu'ils ne connaissent pas. En même temps, commencez à poster car un profil sans post, sans amis et qui a été créé hier, n'est pas exactement sexy. Il est possible de reprendre des profils réels et inactifs, mais c'est encore plus suspect car ici le seul avantage, c'est que le profil a un passé. Mais l'inconvénient, c'est que le contenu ne ressemblera sans doute pas à la personne que vous devez être avec votre faux profil.

Enormément de gens ont un faux profil. Non pas dans le but de nuire ou d'espionner mais tout simplement pour garantir leur sécurité. Ça n'est pas du tout illégal tant que vous n'usurpez l'identité de personne.

b) Identifier les amis Facebook de votre cible

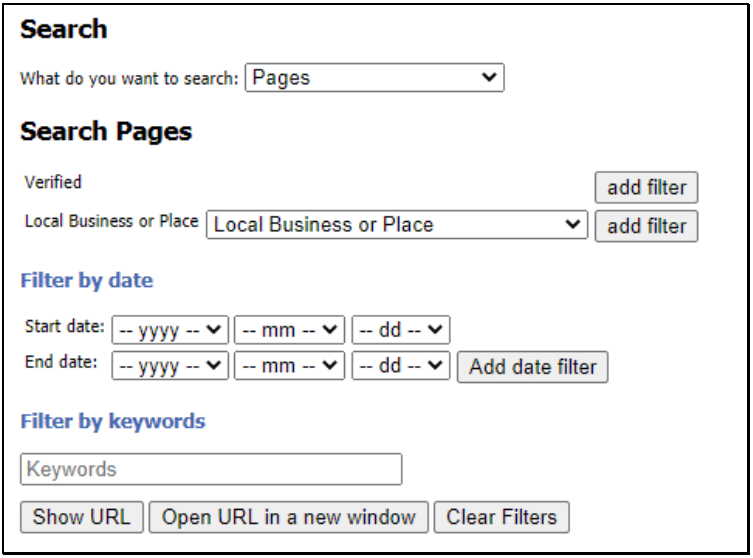
Si vous menez un backgroundcheck sur un futur partenaire commercial, vous avez peut-être envie de connaître ses relations ? Aujourd'hui, beaucoup de gens masquent leur liste d'amis, la laissant éventuellement visible pour leurs proches. Ce qui est totalement inutile. Vous ne pouvez pas cacher vos amis Facebook, sauf si vous ne postez jamais rien.

Pour identifier les amis Facebook d'une cible, vous allez sur chaque publication de votre cible et vous cliquez sur les « like ». En allant sur les différentes publications de la

cible, vous devriez ainsi réussir à obtenir une belle liste d'amis, sans doute pas toute la liste, mais certainement ceux de l'environnement proche.

c) Utilisation d'outils externes pour la recherche sur Facebook

Sowdust est un outil en développement constant. Il permet de mener des recherches Facebook en combinant différents critères. Il permet de mener des recherches chronologiques, de trouver des photos ou des messages publiés ou tagués par une personne, et dans certains cas, de localiser une image.



https://sowdust.github.io/fb-search/

Whoposted permet la recherche d'informations à des dates spécifiques. https://whopostedwhat.com/

FBsearch est un autre outil permettant la recherche sur Facebook. Très simple, mais au fond ne fait rien d'autre que ce que vous pouvez déjà faire via la barre de recherche de Facebook, qui s'est considérablement enrichie.

https://fb-search.com/search

d) Utiliser la reconnaissance de caractères Facebook

Concrètement, s'il est écrit quelque chose sur une photo, un nom, une plaque d'immatriculation, Facebook le trouvera.

Par exemple, si je recherche un véhicule immatriculé « KLT666 », voici le résultat :

Attention, avant que vous ne pensiez retrouver le chauffard qui a éclaté votre voiture, ceci ne fonctionne que si la photo de la plaque existe sur Facebook. La probabilité est faible, même si ça vaut toujours la peine d'essayer.

Dans le moteur de recherche Facebook, vous tapez le numéro d'immatriculation, et ensuite, cliquez sur « photos ».

e) Retrouver quelqu'un sur Facebook par son e-mail ou son numéro de téléphone

Facebook est un excellent outil de recherche d'informations sur les personnes. Avec plus de 2 milliards d'utilisateurs mensuels, les chances de trouver le profil de quelqu'un avec son seul nom de famille sont faibles - d'autant plus que cette personne n'utilise peut-être même pas son vrai nom ou son nom complet ! Heureusement, il existe une autre option : vous pouvez rechercher le profil d'une personne en tapant son adresse électronique ou son numéro de téléphone.

Pour ce faire, il vous suffit de vous connecter à votre profil Facebook et de Saisir l'adresse mail ou le numéro de téléphone de la personne que vous recherchez dans la barre de recherche. Cliquez enfin sur l'onglet "Personnes" en haut de la page.

Ce mode de recherche ne fonctionne que si l'adresse électronique de l'utilisateur, ou son numéro de téléphone, est configuré pour être publiquement visible dans sa section "À propos". Si ce n'est pas le cas, elle n'apparaîtra pas dans les résultats de recherche. Mais ça vaut la peine de tester. De plus, en ce qui concerne le téléphone, vous pourrez très souvent le localiser si la personne a par exemple, une profession de contact, ou un commerce.

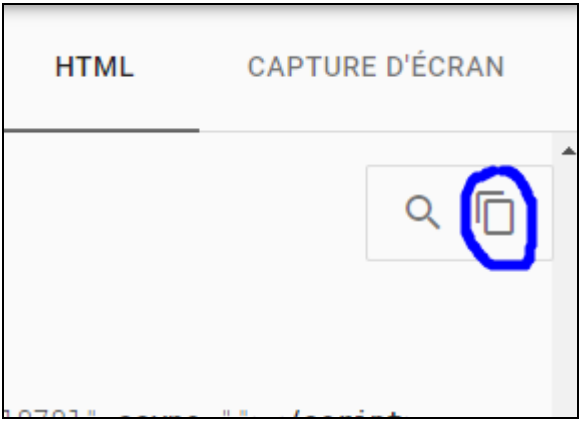
2. LinkedIn

Votre concurrent est-il actif sur LinkedIn ? Probablement. Mais en dehors de ses formidables fonctions de sourcing, LinkedIn est moins intéressant en matière d'analyse compétitive que d'autres sites. Tout simplement parce que votre concurrent ne vend pas ses produits ici. En dehors de l'analyse compétitive, LinkedIn est bien entendu une source d'informations sur les personnes. Vous aurez des données, non vérifiées, sur la scolarité et les différents jobs de la personne. Souvent dans nos métiers, nous ne souhaitons pas être identifié. Or, sur LinkedIn, lorsque vous visitez un profil, la cible sera notifiée de votre passage. Il s'agit d'un paramètre par défaut. Il est possible de modifier vos paramètres pour ne pas être identifiable.

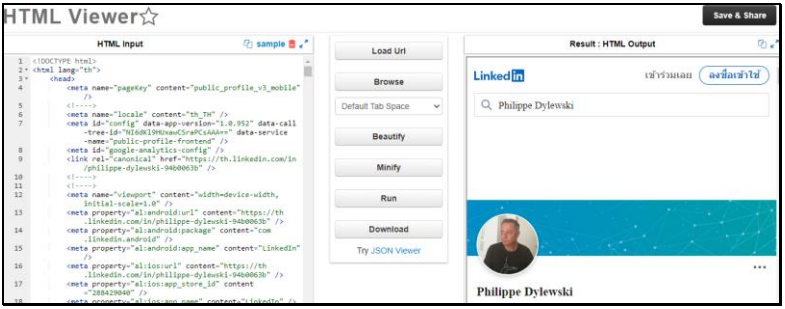
Cliquez sur l'icône « Vous » en haut de la page d'accueil de votre compte puis cliquez sur « Voir le profil », cliquez sur « préférences et confidentialité ». Vous allez sur « confidentialité », dans la section « Comment les autres voient votre activité sur LinkedIn », cliquez sur « options vues de profil ». Une liste déroulante va s'ouvrir, c'est le module « Sélectionner ce que les autres voient lorsque vous consultez leur profil » qui va s'afficher. Vous cliquez sur « Utilisateur LinkedIn Anonyme ». La personne saura que son profil a été visité, mais ne pourra pas vous identifier. Si vous êtes hautement paranoïaque, ou que pour une raison ou une autre vous devez aller régulièrement sur un profil et ne voulez pas éveiller la méfiance de votre cible, il est tout à fait possible de voir un profil sans que la personne ne sache qu'on est venu sur son profil. Cela prend juste quelques minutes.

Pour commencer, vous tapez le nom de votre cible sur votre moteur de recherche habituel, accompagné du mot « LinkedIn ». Vous voyez en tête de page le profil de votre cible. Vous allez sur le titre du lien et vous utilisez le clic droit de votre souris. Cliquez sur « copier le lien ».

Ensuite, vous allez sur https://search.google.com/test/mobile-friendly qui à la base, sert à savoir si une page web est compatible avec votre téléphone. Vous copiez le lien dans la barre de recherche et vous verrez apparaitre le profil LinkedIn de votre cible. Mais comme le profil sera incomplet, vous cliquez sur « html » en haut à droite de la page. La suite de codes qui apparait est peu soluble dans mon intelligence. Difficile à utiliser. Alors, je clique sur le bouton « copier ».



Ensuite, vous ouvrez la page https://codebeautify.org/htmlviewer et vous collez l'information qui se trouve dans le presse-papier. Enfin, vous cliquez sur le bouton « run » et vous obtenez le profil de la cible.



Pour en revenir à votre concurrent, commencez par faire une recherche pour voir s'il possède un compte LinkedIn. Si vous ne le trouvez pas, c’est soit que vous avez mal cherché (recommencez !), soit que votre concurrent n’est pas très dangereux.

Passe-t-il des annonces sur LinkedIn ?

Pour accéder aux annonces d'une page commerciale LinkedIn, allez sur la page et cherchez l'onglet "Ads" à gauche. Cliquez sur cet onglet et vous verrez une liste d'annonces associées à la page.

Notez les annonces qu'il diffuse et voyez ce que vous pouvez apprendre. Passez en revue les créations et les textes que vous voyez pour trouver des idées que vous pouvez intégrer dans vos annonces.

Quelles sont les publicités qui suscitent le plus d'intérêt ?

Vous ne pouvez pas afficher les commentaires ou les interactions sur les annonces LinkedIn directement à partir de la section annonces, mais vous pouvez consulter ces informations de manière détournée.

Cliquez sur les trois points en haut à droite d'un message et sélectionnez "Copier le lien vers le message". Ensuite, collez ce lien dans votre navigateur pour afficher le message en question, ainsi que les commentaires éventuels.

3. Twitter

Quel que soit votre secteur d'activité, vous avez probablement un concurrent sur Twitter. En suivant sa stratégie sur la plateforme, vous pouvez glaner des informations précieuses pour votre stratégie marketing sur les réseaux sociaux, rien qu'en étudiant de près leurs followers.

L'un des meilleurs moyens de savoir ce qui fonctionne pour un concurrent sut Twitter est d'observer ce qu'il fait. Vous n'avez même pas besoin de le suivre directement. Il vous suffit de créer une liste Twitter privée (visible uniquement par vous) et d'y ajouter votre concurrent. Si le concurrent a plus d'un compte Twitter principal, ou si tous ses employés sont sur Twitter, incluez-les également. De cette façon, vous aurez un flux d'informations entrantes vous indiquant exactement comment ils gèrent leur stratégie Twitter.

Vous pouvez créer une liste Twitter privée sur Twitter en sélectionnant "Nouvelle liste" dans la barre latérale de votre page d'accueil. En quelques minutes seulement, vous commencerez à voir le type de contenu que votre liste partage.

En lançant une recherche sur le nom d'utilisateur de votre concurrent, vous pourrez voir les conversations qu'il a avec

ses fans. De cette façon, vous pouvez voir ce que ses fans (ou détracteurs) aiment ou n'aiment pas chez lui.

Vous pouvez créer une recherche dans Twitter en cherchant simplement le nom d'utilisateur de votre concurrent et en utilisant l'option "Enregistrer cette recherche".

Ca vous intéresse d'avoir un aperçu de la liste des clients de votre concurrent ? Bien sur que oui, sinon vous ne seriez pas là. Des services comme Tweepi vous permettent d'afficher la liste de leurs abonnés et de la trier en fonction du nombre de mises à jour, du nombre d'abonnés et d'autres paramètres. Vous pouvez essentiellement découvrir qui sont certains de leurs fans les plus actifs et les plus influents.

https://tweepi.com/

Puisque vous et vos concurrents vous attaquez au même public, suivre leurs mouvements peut être très utile pour élaborer votre propre stratégie.

Vous pouvez obtenir des informations solides en vérifiant à qui parle votre concurrent sur Twitter et dans quelle mesure il est actif sur la chaîne. Par défaut, Twitter vous montre uniquement les tweets sortants de quelqu'un, et non ses réponses. Pour voir les réponses, allez sur son compte Twitter et cliquez sur l'option "Tweets & Replies". Vous pourrez alors voir toutes les conversations qu'ils ont et avec qui. Suivez les personnes à qui ils parlent.

Si vous identifiez certains partenaires clés avec lesquels ils s'engagent régulièrement, faites une recherche à la fois sur votre concurrent et sur ces personnes pour trouver des données historiques sur leurs conversations. Une excellente

tactique est de créer des listes Twitter. Les listes peuvent être publiques ou privées, mais pour surveiller le caractère privé des concurrents, c'est la meilleure solution.

Pour créer une liste via le web :

Cliquez sur l'icône de votre profil pour afficher le menu déroulant.

Cliquez sur « Listes ».

Cliquez sur « Créer une nouvelle liste ».

Sélectionnez un nom pour votre liste, et une courte description de la liste. Choisissez ensuite si vous souhaitez que la liste soit privée (accessible uniquement à vous) ou publique (tout le monde peut s'y inscrire).

Cliquez sur « Sauvegarder la liste ».

Suivre certains hashtags pertinents du secteur peut vous permettre de connaître de nouveaux acteurs sur le marché qui pourraient valoir la peine d'être explorés. Twitter dispose d'une fonction de recherche intégrée située dans le coin supérieur droit de l'écran. Vous pouvez ajouter des opérateurs de recherche avancée - semblables à ceux de Google - à votre requête, plonger en profondeur et retourner des résultats précis. Pour commencer votre recherche dans la base de données de Twitter, il est conseillé d'aller sur la page de recherche avancée de Twitter à l'adresse https://twitter.com/search-advanced. À partir de cette page, vous pouvez personnaliser les filtres de recherche en fonction de plages de dates spécifiques, de personnes et d'autres éléments.

1. (-) est utilisé pour exclure des mots clés ou des phrases spécifiques des résultats de la recherche.

2. Pour rechercher des hashtags, utilisez l'opérateur (#) suivi du mot clé de recherche. Par exemple : #Dior

3.Pour retrouver les tweets postés dans une langue particulière, c'est l'opérateur « lang » qui est à utiliser. Dior lang:fr

4. Utilisez le mot-clé (images) pour renvoyer les tweets qui contiennent une image. Voici un exemple : Filtre OSINT:images (ceci renverra tous les tweets contenant le mot-clé OSINT et contenant une image).

6. Pour renvoyer les tweets contenant une vidéo, utilisez le mot-clé (vidéos). Voici un exemple : Filtre OSINT:vidéos

7. Pour rechercher les tweets avec réactions négatives, utilisez le symbole suivant :(Par exemple : Dior :(retournera tous les tweets contenant le mot-clé Dior avec des attitudes négatives.

8. Limitez vos recherches selon des dates précises avec les opérateurs since: et until:

Exemple : « Dior since:2020-03-01 until:2020-12-31 »

8. Pour rechercher des tweets associant deux propos, vous utilisez l'opérateur AND :

Dior AND:Boston

9. L'un ou l'autre. Vous utilisez l'opérateur OR :

Dior OR:Gucci

10. Filtrer ou exclure. Avec l'opérateur filter:, vous filtrez les tweets selon plusieurs critères :

Verified : afficher les tweets des comptes vérifiés

Follows : afficher les tweets des personnes que vous suivez

Replies : uniquement les tweets de réponses

Retweets : uniquement les retweets

Links : uniquement les tweets avec un lien

Images : uniquement les tweets avec une image

native_video : uniquement les tweets avec une vidéo

Par exemple, pour chercher des liens qui parlent de Dior, utilisez cette requête : « Dior filter:links ».

En utilisant exclude : à la place de filter :, vous excluez les critères ci-dessus.

4. Amazon

Vous perdez des ventes au profit de vos concurrents sur Amazon et vous avez du mal à en comprendre les raisons ? Et si vous pouviez espionner vos concurrents sur Amazon et voir quelles stratégies de prix ils mettent en œuvre pour assurer leur succès ? En utilisant les outils de recherche sur les produits Amazon disponible sur le marché, vous pouvez facilement effectuer une analyse comparative détaillée entre vous et vos concurrents.

Afin de garder une longueur d'avance sur vos concurrents, la première étape consiste à identifier qui ils sont. L'étape suivante consiste à déterminer ce que font vos concurrents, ce qui est souvent un peu plus difficile que de simplement effectuer une recherche sur Google.

Voici quelques facteurs à prendre en compte :

En quoi sont-ils meilleurs ou pires que vous ?

Ont-ils une plus grande variété de produits ?

Quel est leur prix de vente moyen ?

Qu'en est-il de leurs évaluations, de leurs ventes et de leur classement ?

Avec un outil de recherche sur Amazon tel que BigCentral, vous pouvez facilement examiner les performances de votre concurrent en un coup d'œil. Le tableau analytique des meilleures ventes de BigCentral vous donne accès aux performances globales du concurrent avec jusqu'à 120 jours de données historiques, ainsi qu'à son volume de ventes et à ses revenus quotidiens.

Une autre façon d'espionner efficacement les concurrents d'Amazon est de mettre en place une alarme. Le système d'alerte de BigCentral vous informera automatiquement de toute modification de l'inventaire, du prix, des avis, des évaluations, des revenus et autres de votre concurrent.

BigCentral, c’est bien. Vous pouvez l’essayer pendant deux semaines. Mais à 50 dollars l’abonnement de base, il faut que votre présence sur Amazon soit autre chose que la vente de trois bouquins d’occasion par mois.

https://www.bqool.com/

Une autre raison importante de surveiller activement les concurrents d'Amazon est de découvrir quels produits de votre concurrent vous grignotent vos revenus. Vos concurrents ne sont pas seulement ceux qui vendent les mêmes produits que vous, mais aussi d'autres vendeurs qui vendent des produits qui peuvent être achetés en complément de ce que vous vendez. Il est donc essentiel que vous suiviez les performances des produits de votre concurrent.

Avec le suivi des produits, vous pouvez facilement identifier les produits les plus vendus de votre concurrent et surveiller le prix du produit, les avis, les ventes, la marge bénéficiaire et le montant des stocks. Grâce à cette analyse approfondie, vous pouvez mettre en œuvre des plans d'action pour devancer vos concurrents.

La fonction ASIN inversée vous indique les mots clés que vos concurrents utilisent déjà avec succès, le volume de recherche, les ventes moyennes, le taux de clics et des mesures de performance. L'Amazon Standard Identification Number (ASIN, littéralement « numéro d'identification standard Amazon ») est un code d'identification de produit utilisé par Amazon.com. Chaque produit vendu par Amazon et ses filiales est doté d'un numéro ASIN unique (définition, Wikipédia).

Trendle vous aide dans cette mission avec un budget raisonnable, allant de la gratuité pour deux semaines à un abonnement qui commence à 10 dollars par mois.

https://trendle.io/

Comment pouvez-vous découvrir quand vos concurrents organisent des promotions ? Voici quelques moyens :

Consultez la rubrique "Offres du jour" sur Amazon.

Visitez le site web de votre concurrent pour voir s'il propose des réductions ou des offres.

Vérifiez sur les médias sociaux, les blogs, les newsletters, les affiliés, etc. De nombreux vendeurs publient également leurs offres spéciales sur des pages de fans.

Amazon est un endroit très compétitif et sans pitié. Vous perdez une longueur d'avance en très peu de temps. Vos concurrents vous surclassent en quelques heures. Vos clients célèbrent votre gloire ou vos déboires en deux clics. S'il y a bien un endroit où l'information est une question de survie, c'est bien sur Amazon.

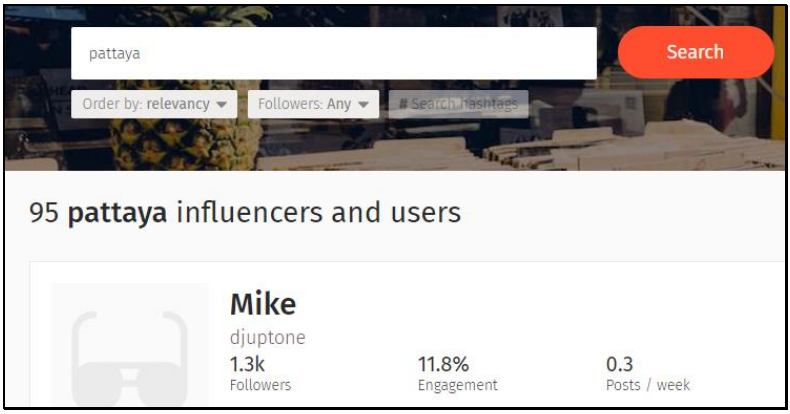
5. Instagram

Instagram, c'est le réseau social de l'image, que ce soient des photos ou des vidéos de courtes durées. A la base, aucun intérêt pour le renseignement. Espionner des ados en train de faire semblant de s'amuser au bord d'une piscine n'apportera pas grand-chose à vos analyses concurrentielles. Aujourd'hui, Instagram est devenu un indispensable pour les marques et les entreprises. C'est l'endroit pour se faire connaître et reconnaître. Nous avons déjà vu comment faire le suivi des pubs sur Instagram. Il reste deux autres catégories importantes : les followers et les influenceurs.

Les followers sont ceux qui ont décidé de suivre un utilisateur. Ils nous intéressent car ils sont le véritable poult d'une marque ou d'une entreprise. Nous nous intéressons à ce qu'ils aiment, ce qu'ils n'aiment pas, ce qu'ils en disent et qui ils sont.

Un influenceur est une espèce d'intermédiaire star entre une marque et son public. Du fait de sa notoriété, l'influenceur a le pouvoir de « guider » les consommateurs dans la bonne direction. Il a bien plus de crédibilité qu'une campagne de pubs car le facteur confiance joue en sa faveur.

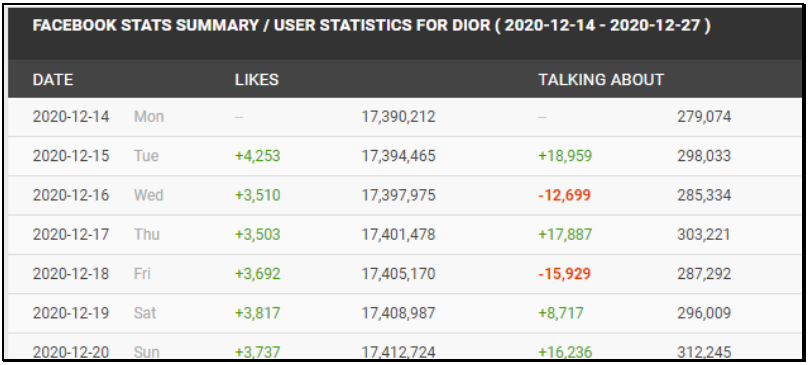
Par exemple, si mon client est un tour operateur qui organise des voyages sur la rayonnante cité de Pattaya, Thaïlande, je voudrai connaître les principaux influenceurs liés à ce sujet. C'est ce que fait gratuitement Searchmybio.



Pour chaque recherche thématique, j'obtiens une liste des principaux influenceurs. Avec leur nombre d'abonnés, le taux d'engagement (pourcentage des abonnés qui interagissent avec une publication) et le nombre de posts par semaine.

https://www.searchmy.bio

Avec Social Blade, je peux suivre mes concurrents sur Instagram et tout connaître de leur évolution quasi en temps réel : nombre de followers, taux d'engagement, les pages suivies par la marque, le nombre moyen de likes et de messages, le tout accompagné de graphiques très clairs. Ce qui est très intéressant avec Social Blade, c'est que le site fait le même job pour d'autres réseaux sociaux comme Facebook, YouTube, Twitter ou 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. Tout savoir sur vos partenaires commerciaux

Ce sont vos clients, vos agents, vos distributeurs, un projet de fusion ou d'acquisition.

Pour l'essentiel, les méthodes sont identiques à ce que vous trouvez dans le chapitre consacré à l'information sur vos concurrents. Je vous recommande la lecture de ce chapitre, vous y trouverez une série d'outils qui vous seront utiles pour votre projet.

Cependant, il y a des différences. Si votre concurrent est en difficulté financière ou se traine une réputation de voyou, vous n'y voyez aucun inconvénient. Dans le cas d'une alliance, c'est un problème rédhibitoire.

Grace aux bases de données, vous obtenez toute l'information sur les finances de l'entreprise, ses crédits, ses délais de paiements…Bien sûr, l'analyse financière est indispensable. Vous avez étudié sa stratégie marketing et c'est parfait.

Toutes ses informations ont un point négatif commun : elles vous donnent de l'information sur le passé de l'entreprise. Quand vous lisez un bilan, il s'agit d'un bilan appartenant au passé. Il ne vous dit pas ce qui se passe aujourd'hui. Bien sûr dans le cas d'une reprise, vous avez tout loisir de demander les résultats intermédiaires de l'année en cours. Mais vous-même avez déjà dans le passé arrangé vos résultats pour qu'ils paraissent le plus joli possible. On ne parle pas de fraude, non, tout de suite les grands mots. On parle d'embellissement. Vous avez fait le déplacement pour

visiter l'entreprise et constater son dynamisme. Mais votre futur partenaire était prévenu de votre visite. Vous, quand vous recevez des gens importants, vous mettez les petits plats dans les grands, non ? Eux aussi. Des intérimaires ont pu être engagés pour la journée. La famille et les amis se sont bousculés toute la journée pour donner l'impression que les clients dépensaient en masse. Le téléphone n'arrête pas de sonner. Les camions vrombissent. Les machines tournent à en devenir rouges. Les réseaux sociaux clament à quel point votre futur partenaire est un joyau.

Ce type d'arnaque était l'une des plus populaires en Thaïlande jusqu'au début 2020. Des milliers de francophones arrivaient chaque année au Pays du Sourire avec le rêve de se construire une nouvelle vie au soleil. Reprendre un petit commerce, un hôtel, un bar ou un restaurant. Le pigeon cherche à entrer en contact avec des francophones installés dans le pays depuis longtemps. Il fait chaud, l'ambiance est tellement sympa. Très vite, il sera informé que justement, un super bar est à remettre car le propriétaire veut rentrer en France pour des raisons familiales ou de santé. Le rendez-vous est pris dans le bar en question. Et c'est la folie. On doit pratiquement pousser les billets de banque dans la caisse avec le pied. C'est la fête, tout le monde s'amuse, les gens consomment sans compter. Le pigeon est appâté, il a trouvé l'affaire du siècle, il est traité comme un roi, présenté à la clientèle comme le futur proprio. Il n'a jamais vu ça. Il y a bien un prix de reprise conséquent et un bail à reprendre, mais ça reste acceptable. Après deux ou trois beuveries où le pigeon se voit déjà en prince de la nuit, l'affaire est rondement menée. Tout se passe formidablement bien jusqu'au jour de

l'ouverture. Car le jour de l'ouverture, il y a tout juste trois clients perdus. Vers 23H00, une patrouille de police arrive, et signale au pigeon qu'il n'est pas en ordre de ceci et cela. Il comprend vite qu'il faut payer. Pas des masses car ici on ne tue pas le pigeon, on le cuit à feu doux. Le vrai problème n'est pas la corruption, car au fond ça n'est jamais qu'une modeste contribution aux œuvres de la police et votre sécurité est garantie. Le vrai problème, c'est que tous ces fêtards ne sont pas là. Et pour cause puisqu'ils bambochent dans le nouvel établissement ouvert par l'ancien propriétaire. Qui se fera un plaisir de rendre service au pigeon, en lui reprenant son établissement tout neuf pour une somme fort modeste.

Vous pensez qu'on ne peut pas vous avoir avec des balivernes pour attardés en mal d'aventure ? Alors vous vous ferez avoir. J'entends déjà des bruits de roucoulement. Ciel, serait-ce un pigeon ? La seule façon de ne pas se faire avoir, c'est d'avoir l'humilité de reconnaître que c'est possible.

Ce que vous pouvez difficilement savoir, c'est si un évènement important s'est produit pour votre potentiel partenaire ces derniers mois. Mais c'est possible.

Que votre futur partenaire soit dans votre pays ou à l'étranger ne change pas grand-chose. La seule différence, c'est QUI fera le job de renseignement.

a) S'il s'agit d'un commerce accessible au public

- Envoyez quelques personnes se faire passer pour des clients en semaine et le weekend.

- Vérifiez que les personnes clés sont toujours bien en place. Par exemple, que ce restaurant dont vous envisagez la reprise n'a pas vu son chef démissionner pour ouvrir son propre établissement à proximité. Ou que le propriétaire va ouvrir une nouveauté dans le quartier.

- Quelqu'un se mettra en planque pour observer le nombre d'entrées sur une journée dans l'établissement. Un jour de semaine et un jour de weekend. Cette personne comptera le nombre de sacs et comptabilisera le chiffre d'affaires supposé avec ces informations. Au passage, je vous signale que c'est exactement ce que font certains fonctionnaires des finances.

- Le responsable de l'enquête fera son tour dans l'environnement immédiat du commerce et cherchera à engager la conversation avec les habitants du quartier. Une personne clé sera le facteur car il sait tout. Jusqu'il y a quelques années, beaucoup d'agences immobilières payaient des facteurs pour être au courant d'affaires potentielles. Bon, peut-être que ça se fait encore.

- Vous menez une enquête approfondie sur le propriétaire via les réseaux sociaux, la presse et les médias en général.

- Si possible, vous contactez les fournisseurs du commerce sous un quelconque prétexte, pour avoir des informations sur les habitudes de paiement de la cible.

- Enfin, via un détective privé, vous investissez une petite somme pour tout connaître du patrimoine et de la solvabilité en temps réel du propriétaire.

- Normalement, vous n'avez pas accès au casier judiciaire, mais savoir qu'il a été condamné il y a 25 ans pour avoir vendu de l'herbe ou volé une voiture n'est pas d'un grand intérêt. S'il a commis un délit sérieux ces dernières années, vous devriez en avoir une trace dans les médias.

b) S'il s'agit d'une plus grande entreprise ou d'une entreprise non-accessible au public

- Certains des points précédents sont de mise : enquête de solvabilité PERSONNELLE du ou des dirigeants, contacter les fournisseurs, tester le produit/service, la qualité de l'accueil, vérifier que les principaux responsables n'ont pas de projets incompatibles avec le vôtre…

- S'il y a de la production, comptez sur un ou deux jours ce qui sort de l'entreprise. Profitez-en pour être attentif à l'état des camions.

- Si c'est de la prestation de services, contactez des clients pour savoir si des modifications de prestations sont apparues récemment.

- Lorsque vous vérifiez la réputation de l'entreprise sur les réseaux sociaux, soyez particulièrement attentif à la date de publication. Car si le propriétaire

cherche à donner une image fausse, de nombreux posts anormalement positifs seront très récents.

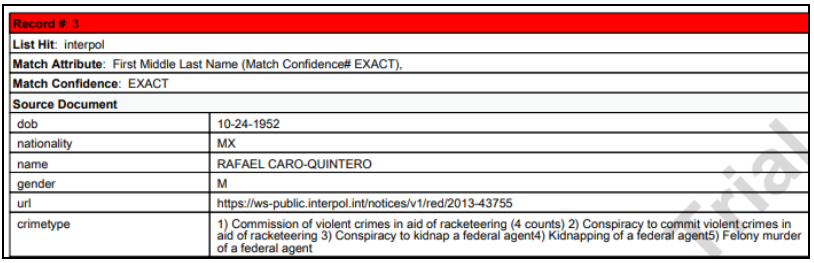
- Durant le temps de midi, envoyez quelqu'un dans les endroits où des membres du personnel prennent leur lunch et soit juste écouter les conversations, soit si l'enquêteur est habile, s'y mêler.

- Vérifiez sur LinkedIn que certains cadres clés n'ont pas pris la clé des champs ces derniers temps. Cela se fait en faisant une recherche sur les personnes qui travaillent ACTUELLEMENT dans l'entreprise ou bien qui y ont travaillé. Si vous voyez que des gens ayant travaillé pour l'entreprise ont changé massivement d'emploi ces trois derniers mois, un signal d'alarme devrait commencer à se faire entendre dans votre tête.

- Si vous projetez un partenariat avec une entreprise possédant filiales et magasins, pensez à y organiser des visites et regarder si de nouvelles entreprises concurrentes ne se sont pas récemment installées dans le coin.

- Vous n'avez certainement pas envie de travailler avec une entreprise ou des gens suspectés de financer le terrorisme, interdits bancaires, se retrouvant sur des listes internationales de blanchisseurs d'argent sale, fugitifs recherchés par Interpol, dont les avoirs sont gelés dans divers pays, ou sur la liste des criminels recherchés par le FBI. Ce serait fâcheux pour votre business. Les organismes financiers sont obligés de vérifier que

leurs clients sont de braves clients. Il existe à travers le monde des centaines de listes reprenant les noms d'individus fort peu recommandables. Il ne vous est pas possible d'en faire le tour, car vous en auriez pour des semaines. Heureusement, de nombreuses sociétés se chargent de centraliser l'information pour vous. Souvent à des tarifs de gangsters. KYC2020 est le bon élève de la classe. Non seulement vous pouvez tester leurs services gratuitement, mais après l'essai, leurs prix sont fort compétitifs. Le rapport PDF que vous recevez vous donne une réponse simple : oui ou non. Ensuite, le document vous explique pourquoi il n'est pas opportun de travailler avec ce sympathique homme d'affaires avec qui vous envisagiez une solide coopération.



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

C'est avec stupeur que j'apprends que Rafael est recheché par la plupart des polices de la planète pour racket, meurtres, conspiration et kidnapping. Vous ne pourrez plus dire que vous ne saviez pas.

https://www20.kyc2020.com/

Tant que vous y êtes, vérifiez aussi sur la liste des criminels les plus recherchés d'Europe via le site d'Europol.

https://eumostwanted.eu/fr

Le site du GTD (Global Terrorism Database) est le plus grand répertoire du monde en lien avec des évènements terroristes puisqu'il répertorie près de 200.000 attentats depuis 1970. Vous y trouverez le nom de toute personne impliquée et identifiée.

https://www.start.umd.edu/gtd/

Le UNITED NATIONS SECURITY COUNCIL propose un moteur de recherches de gens ou organismes affiliés au terrorisme international.

https://scsanctions.un.org/search/

XI. Le Dark Web

Le dark web désigne les contenus en ligne cryptés qui ne sont pas indexés par les moteurs de recherche classiques. Le dark web fait partie du web profond, qui se réfère simplement aux sites web qui n'apparaissent pas sur les moteurs de recherche.

Des navigateurs spécifiques, tels que Tor, sont nécessaires pour accéder au web profond. De nombreux sites du dark web fournissent simplement des services standards avec un anonymat accru, ce qui profite aux dissidents politiques ou aux personnes en général qui essaient de garder leur vie privée. Evidemment, la vente illégale de drogues ou de médicaments, le porno pour tous les gouts, les données volées vendues aux enchères et les armes attirent le plus l'attention du grand public. Le dark web fait autant rêver que frémir.

https://www.torproject.org

Le projet Tor est une organisation à but non lucratif qui mène des recherches et des développements sur la vie privée et l'anonymat en ligne. Il est conçu pour empêcher les gens - y compris les agences gouvernementales et les entreprises - de connaître votre position ou de suivre vos habitudes de navigation.

Sur la base de ces recherches, Tor propose une technologie qui fait rebondir le trafic des internautes et des sites web par des "relais" gérés par des milliers de bénévoles dans le monde entier, ce qui rend extrêmement difficile pour quiconque d'identifier la source de l'information ou la localisation de l'utilisateur.

Son logiciel peut être téléchargé et utilisé pour tirer parti de cette technologie, une version séparée étant disponible pour les smartphones Android. Comme lors des débuts d'internet, le dark web a également acquis une réputation de refuge pour les activités illégales. Réputation fondée, mais seulement en partie car le dark web est aussi un lieu de préservation de la vie privée -et ce livre vous démontre à quel point elle est fragile-.

Une grande partie du contenu du dark web est très amateur. C'est peut-etre aussi ça qui le rend fascinant, un peu comme l'adolescence. Le dark est encore en pleine évolution, et ses coûts et avantages ne sont pas encore connus dans leur intégralité.

Le dark web, comme internet avant lui, est souvent accusé de crimes horribles, tels que la maltraitance d'enfants et les meurtres sur commande. Cependant, ces crimes existaient bien avant l'Internet ou le dark web. La différence, et elle de taille, c'est qu'avec le dark web, il est plus facile de ne pas se faire prendre. Il est essentiel d'éviter de confondre le dark web avec les cryptomonaies souvent utilisées pour y effectuer des achats. Le dark web facilite la création et l'accès à des sites web offrant un degré élevé d'anonymat pour toutes les personnes concernées. Beaucoup de ces sites ne contiennent que des informations, sans possibilité d'acheter ou de vendre quoi que ce soit. Il est vrai que des cryptomonaies, telles que le Bitcoin, sont souvent utilisées pour les transactions sur le dark web. Cependant, il n'est pas nécessaire d'utiliser le dark web pour utiliser des cryptomonaies.

Le dark web et le deep web sont aussi souvent utilisés de façon interchangeable et erronée. Le deep web comprend toutes les pages qui n'apparaissent pas lorsque vous lancez une recherche sur le web. Le dark web n'est qu'une partie du deep web, qui contient également tout ce qui nécessite une connexion, comme les services bancaires en ligne, les sites de paiement et les services d'hébergement de fichiers. Le dark web est un sous-ensemble du deep web qui est intentionnellement caché, nécessitant un accès par un navigateur spécifique.

Wikipédia affirme que le dark web contient 500 fois plus d'information que le web indexé. Possible. Mais comme c'est caché, difficile de faire ce genre d'estimation. Et pour définitivement couper court aux fantasmes, retenez bien ceci : le dark web, c'est juste ce qui n'est pas indéxé par Google. L'essentiel du contenu de Facebook ne l'est pas. Le web profond, ce sont les informations financières, les catalogues d'achats, les horaires de vols, la recherche médicale et toutes sortes d'éléments stockés dans des bases de données qui demeurent totalement inaperçues par les moteurs de recherche. Le contenu d'un portail n'est souvent pas indexé. Ce qui ne veut pas dire que les informations ne sont pas accessibles. Car elles le sont. Ceci étant dit, le dark web, c'est quand même entre 60 et 70 % d'activités illégales, en tout cas d'après une étude de l'Université du Surey datant de 2016.

Pour les amateurs, Des kits de rançon sont disponibles sur le dark web depuis plusieurs années, et ces offres sont devenues beaucoup plus dangereuses avec la montée de groupes criminels spécialisés qui développent leurs propres logiciels malveillants, parfois combinés à des outils

préexistants, et les distribuent par l'intermédiaire de "filiales".

Ces attaques consistent souvent à voler les données des victimes et à menacer de les diffuser si la rançon n'est pas payée. La différence entre cette méthode et les mails que je reçois chaque semaine, m'informant que des photos de moi totalement nus seront diffusées si je ne paie rapidement, c'est qu'avec les outils achetés sur le dark web, nous n'en sommes plus au stade de la simple menace spamée à des millions d'exemplaires, mais à une attaque ciblée et équipée. Nous sommes dans l'industrie du crime virtuel, et comme ils sont couverts par les multiples protections qu'offrent le dark web, ils ne sont pas prêts de se faire prendre.

Ca y est, vous venez d'installer Tor et vous en salivez déjà. Vous voyez une jolie barre de recherche et vous vous dites que c'est bien plus facile que vous ne le pensiez. Vous commencez à taper des mots obscurs dans l'espoir de tomber sur des sites déments et vous constatez que tout ce que vous trouvez, vous l'auriez trouvé avec Google. Car jusque là, vous utilisez simplement DuckDuckGo, le moteur de recherche intégré à Tor. Tout ce que vous avez jusque là, c'est un surf anonyme. TOUS les sites du dark web se terminent en .onion. Pas de .fr, ni de .com, rien que des .onion.

Cela veut donc dire que Tor ne sert à rien à part surfer discrètement ? Quelle déception ! Rassurez-vous, chers 007 du net, ça n'est pas le cas du tout. Si Tor ne vous permet pas d'accéder au dark web, il est cependant indispensable pour aller y faire un tour. Quand vous avez trouvé une

adresse.onion, vous la lancez dans le moteur de recherche de Tor, et vous partez en voyage au pays du dark web. Il n'y a pas vraiment de moteur de recherche du dark web comme Google. Nous sommes dans un monde d'anonymat, vous vous attendiez à de la pub avec des hollogrammes ? Le dark wek n'a jamais eu pour vocation d'être organisé ou indexé.

Bien sûr qu'il y a des moyens de trouver des listes de sites. Mais ne négligez pas qu'ils peuvent disparaitre d'un jour à l'autre.

Comment trouver des sites .onion ?

Pour rappel, vous n'y avez accès que via le moteur Tor.

Hidden Wikki est une version "dark web" de Wikipédia où vous pouvez trouver des liens vers différents sites sur le dark web. Comme vous pouvez le remarquer, de nombreux liens en oignon semblent absurdes, car ils sont constitués d'une combinaison de nombreux chiffres et lettres aléatoires. Il est donc difficile de trouver le site web que vous recherchez. Hidden Wikki fait une grande partie de la recherche pour vous.

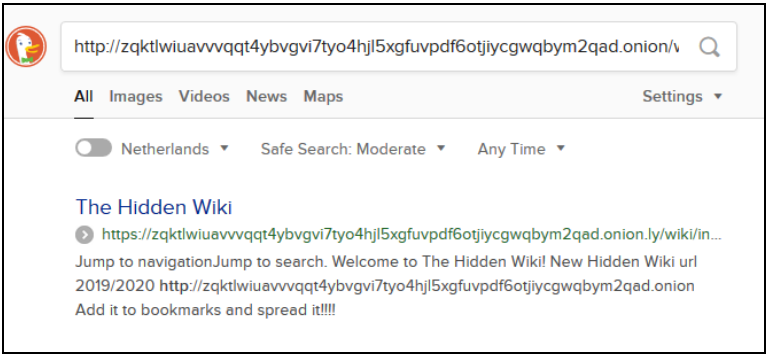
Soyez toutefois prudent. Veillez à ne pas cliquer sur un lien vers quelque chose que vous ne voulez pas voir, car Hidden Wikki ne se contente pas d'indexer les sites web légaux. En fait, il existe de nombreux sites "Hidden Wiki" différents. Le Hidden Wiki était connu pour héberger, ou du moins indexer, un certain nombre de sites web pédophiles et a donc fait l'objet de cyber-attaques de la part du FBI et d'Anonymous. De nombreux imitateurs et dérivés du Wiki

caché ont également été créés. Ne soyez pas surpris si vous tombez sur plusieurs versions du Wiki caché "The Official" ou "The Uncensored". Si vous tapez « Hidden Wiki » sur Tor, c'est ce qui se passera.

Ceci est l'adresse du site original :

http://zqktlwiuavvvqqt4ybvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbym2qad.onion/wiki/index.php/Main_Page

Si vous avez uniquement la version papier de ce livre, ça va être compliqué. N'oubliez pas de lancer l'adresse uniquement avec Tor. De toute façon, si vous tentez le coup avec Google, ça ne marchera pas.



En voici quelques autres. Les sites disparaissent très vite, donc si ça ne marche pas, inutile de m'envoyer un mail cinglant, passez au suivant :

http://3g2upl4pq6kufc4m.onion

http://hss3uro2hsxfogfq.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

Aucun de ces liens n'est à proprement parlé un moteur de recherche. Cela s'apparente davantage à des listes de liens.

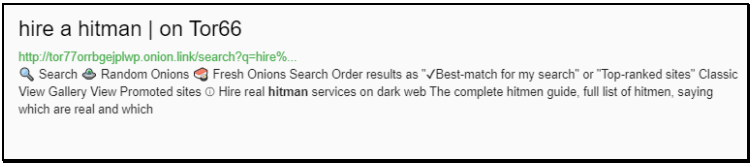
Si vous voulez en trouver d'autres, vous pouvez utiliser Google avec des expressions comme « onion links »,

« darkweb links » ou « dark web onion ». Vous trouverez alors des milliers de liens que vous utiliserez via Tor.

Avant de vous aventurer sur ce terrain, sachez que vous êtes en sécurité en passant par Tor. Mais vous ne l'êtes plus une fois sur le terrain car une fois sorti de Tor et que vous êtes sur un site du Dark Web, votre adresse IP devient visible et identifiable. Vous aurez besoin d'un bon antivirus et d'un VPN.

Vous constaterez que votre navigation est ralentie. C'est normal. Chacune de vos requêtes est envoyée à un serveur, qui le renvoit à un autre, qui… et assure votre anonymat.

Enfin, si vous recherchez la collaboration d'un hacker, c'est ici que vous la trouverez. Tapez simplement « hack » ou « spy » sur Tor, et vous serez immédiatement mis en contact avec des centaines de prestataires venant de tous les pays.



Histoire de vous montrer à quel point le dark web est un endroit décomplexé, ci-dessus vous trouvez un site qui non seulement vous permet de trouver un tueur professionnel, mais qui en plus donne des informations sur le niveau de performances de la personne en question. Je n'ai aucune idée si ce site est sérieux ou pas, ce n'est pas ce qui est important. Ce que je voulais vous montrer, c'est que si vous voulez quelque chose, le dark web l'a.

https://darksearch.io/ se veut le premier moteur de recherches du dark web. Belle ambition. Intéressant. Mais propose tellement de liens brisés que ça peut énerver.

XII. Organiser planques et filatures

Je crois bien que les deux activités les plus ingrates pour un enquêteur sont les planques et les filatures. Je me souviens très bien de ma dernière planque, c'était un soir de Saint Valentin et j'étais scotché à un lampadaire en attendant que quelqu'un vienne rendre visite à ma cible. Les lumières se sont éteintes un peu avant minuit, j'ai attendu encore une heure dans le froid, et je suis rentré chez moi où ma copine ne se trouvait pas.

Vous rentrez dans le renseignement, qu'il soit privé ou d'état, parce que vous avez vu des tas de films et que vous révez de vivre comme vos héros. Je n'ai pas été déçu par le job, il m'a donné ce que j'en attendais et bien plus. Mais suivre quelqu'un c'est chiant et stressant. Une planque, c'est chiant et stressant. Filer et planquer sont les deux activités que l'on pratique quand on a aucun autre choix.

Je sais que ça a l'air débile, mais l'influence du cinéma est profonde dans ces deux activités. Si le cinéma filmait la réalité, personne n'irait voir un film. Qui a envie de voir un détective se faire griller à un feu rouge ou mourant d'envie de pisser alors que ça fait dix heures qu'il observe la même porte ?

Voyons comment nous pouvons organiser tout ça…

1. La filature

Nous allons voir les différentes étapes pour organiser votre filature au mieux, ainsi que les situations à envisager. Avant de mettre votre plan à exécution, pensez que suivre quelqu'un peut relever du harcèlement.

a) Planification

Ne vous lancez jamais dans une surveillance sans avoir d'abord fait vos devoirs. Plus vous en saurez sur les habitudes et les actions de votre cible, plus vous serez à même de la suivre. Vous ne pouvez pas espérer suivre quelqu'un sans préparation.

Avant de démarrer, vous devez pouvoir répondre aux questions suivantes à propos de votre cible :

- Adresse privée et lieu de travail
- Emploi du temps
- Véhicule et immatriculation
- Habitudes
- Et bien sûr, son apparence

Beaucoup de questions trouvent une réponse grâce aux réseaux sociaux. Que vous deviez prendre la cible en filature au départ de son domicile ou de son travail, utilisez un outil de cartographie pour étudier le quartier et pour déterminer les itinéraires que votre suspect pourrait emprunter et aussi identifier racourcis et sens interdits.

Si votre filature démarre d'une entreprise, vous devez connaître les différentes sorties et identifier laquelle est la plus souvent prise par la cible.

Comme vous ne pourrez probablement pas travailler seul, il vous faudra des talkies walkies ou des micro-émetteurs espion, qui pour ce genre de job, sont bien mieux qu'un téléphone portable car vous ne perdez pas de temps à former un numéro et que la communication ne coupe pas dans les tunnels. Pensez à acheter un matériel un peu sérieux, et pas le gadget que vous avez offert aux gosses pour Noël.

Si la filature démarre en voiture, posez un tracker sur le véhicule de la cible. Cela ne vous dispensera pas d'une filature, car vous ne savez jamais quand elle va descendre de voiture, mais cela fera diminuer un peu le niveau de stress.

Durant cette étape, vous vérifiez que votre matériel fonctionne et que vous n'allez pas tomber en panne d'essence.

b) Apparence

Dans la vraie vie, James Bond n'aurait pas pu être enquêteur de terrain. Son personnage représente exactement ce qu'un enquêteur ne doit jamais être.

- Portez toujours des vêtements qui ne se distinguent pas ou qui n'attirent pas l'attention. Le look idéal sera celui de l'endroit où vous allez travailler. Si vous commencez une filature pédestre dans un

quartier d'affaires, vous ressemblerez à un cadre. Si elle démarre dans un quartier pourri, vous aurez le look déglingué qui va avec les murs du coin.

- Si vous êtes très beau ou très laid, c'est un gros inconvénient car vous vous ferez remarquer. De même si vous êtes de n'importe quelle minorité ethnique dans un endroit où il y en a peu.

- PAS de lunettes de soleil. Sauf si c'est l'été et que d'autres gens en portent dans l'environnement immédiat.

Nous reconnaissons les gens non pas à des détails mais à des périphériques. Si vous avez l'habitude de cottoyer une personne en uniforme, la première fois que vous voyez cette personne habillée en civil, il vous faudra sans doute un petit temps avant de la reconnaître. Les périphériques d'identification sont la démarche, l'allure générale, les lunettes, chapeau, sac, vêtements, coiffure, forme générale du visage.

Vous pouvez être quasi invisible pour votre cible en modifiant régulièrement vos périphériques. Un moment vous portez une casquette, l'heure d'après non. Vous avez une veste réversible bleue d'un côté et verte de l'autre. Des lunettes neutres un moment, pas de lunette durant un moment. Idem pour tous les périphériques. Y compris la démarche, qui est un très gros facteur d'identification périphérique. Je ne vous recommande ni le maquillage ni la perruque, sauf si vous travaillez avec de vrais professionnels.

c) Filature

Le plus souvent, vous suivez une cible qui se déplace en voiture ou à pieds. Mais il y a aussi les motos, vélos, et transports en commun (bus, métro, train, avion).

La voiture

Suivre une cible sur une autoroute n'est pas très compliqué. A moins d'être débile, vous gardez une bonne distance avec la cible, et tout devrait bien se passer. Vous savez que la cible est en voiture maintenant, vous ignorez quand elle va descendre du véhicule. Et c'est là que toute la différence avec le cinéma commence. Vous devez au minimum être deux pour une filature voiture. Le conducteur et le « piéton », celui qui quittera la voiture en même temps que la cible. Dans un film, le héro trouve une place de parking en une seconde. Dans la réalité, le temps que vous en trouviez une, la cible est déjà loin. Le « piéton » sert à éviter ça. En ville, sans traceur sur le véhicule cible, une filature avec une seule voiture est quasi impossible. C'est mort au premier feu rouge. N'importe quel évènement vous fait perdre la cible en 30 secondes. Raison pour laquelle, une filature pro se fait avec 3 véhicules et une communication radio constante. Votre véhicule suit la cible, un deuxième suit le même axe sur une voie parallèle à votre gauche, tandis que le troisième fait la même chose à votre droite. Dès que la cible change de direction, un autre véhicule prend le relais et la structure de déplacement se remet à l'identique. C'est chouette, non ? 3 voitures, minimum 6 personnes engagées dans l'opération. Seuls les services d'état peuvent s'offrir ça. Un privé ne parviendra

que très rarement à convaincre un client de débourser ce qui est nécessaire. Car le client aussi a vu Starsky et Hutch. En cas d'accident ou de retrait de points sur votre permis, le client s'en lavera les mains.

Avant de démarrer, assurez-vous d'avoir un plein réservoir d'essence, des snacks et toutes les fournitures dont vous pourriez avoir besoin. Si vous utilisez du matériel, comme des jumelles de surveillance ou des caméras vidéo, prévoyez des batteries de secours supplémentaires et testez le matériel avant de partir.

Si vous êtes en dehors d'une grande ville, vous risquez bien moins de perdre votre cible, mais par contre vous augmentez vos chances d'être repéré. La voiture de James Bond, vous oubliez. Quoi que je connaisse un détective qui travaillait avec une Mercedes jaune. Votre voiture est tout ce qu'il y a de plus banale. Si votre cible n'a aucune raison de se méfier, vous avez une chance. Si elle est un peu sur ses gardes, une filature hors ville avec un seul véhicule est hautement improbable.

En moto

En ville, la moto est un excellent moyen pour filer une cible. Vous pouvez vous faufiler dans les embouteillages et rester quasi invisible de la cible en restant dans son angle mort. Si la cible change subitement de moyen de transport, il est plus simple de garer une moto qu'une voiture. Si en plus, vous avez un collègue à l'arrière, c'est encore mieux car votre binome poursuit la filature à pieds tandis que vous restez mobile et prêt à reprendre le job. Mais c'est très

dangereux et les risques d'accidents sont très élevés. Conduire une moto en temps normal est déjà un excercice qui demande toute votre attention. Etre attentif à l'environnement ET à votre cible n'est envisageable que si vous avez une très grande expérience de la moto.

Hors de la ville, la moto n'est pas un avantage car vous serez très vite repéré, ne fut-ce qu'avec le faisceau de votre phare.

A pieds

Quand vous suivez quelqu'un dans l'espace public, vous ne regardez JAMAIS la cible. Je crois qu'il s'agit là de la plus grosse erreur commise par les amateurs. Si votre regard croise celui de la cible, c'est terminé, vous êtes grillé. Vous gardez la cible dans votre champs de vision mais en regardant à gauche ou à droite d'elle.

Votre rythme est celui de la rue. Vous courez ? Vous êtes identifié, idem si vous marchez trop vite. Le bon sens est votre ami. Vous ne pouvez pas suivre votre cible partout. Si par exemple, elle rentre dans un grand magasin et se ballade au rayon des sous-vêtements, vous n'y allez pas.

Utilisez les vitrines de magasins pour voir sans être vu. Un type seul sera plus vite repéré qu'une femme seule. Un couple, c'est encore mieux. Un chien c'est très bien. Pour ma part, j'ai fait de nombreuses filatures avec mon fils quand il était petit. Qui va imaginer qu'un type qui se balade avec son gosse est un enquêteur ?

Allez, un peu de glamour quand même. Si vous travaillez en équipe, ce qui est une très forte suggestion, vous devez communiquer entre vous de façon rapide, précise et compréhensible. Pas du tout la façon dont vous parlez habituellement avec vos amis. Dire que la cible tourne à droite ne veut rien dire. La droite de qui ? Vers où ?

« la cible part en direction du magasin la Brise d'Eté. Je répète, la Brise d'Eté. Over. »

Votre collègue doit répéter l'information pour la confirmer. C'est de la communication sécurisée et pour communiquer comme un pro au téléphone ou avec walkie, c'est un must.

La cible porte un nom de code. Chaque membre de l'équipe aussi. Pas pour faire joli, mais parce que c'est pratique.

Au téléphone, les sons ne passent pas si bien que ça. Il y a souvent 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	

Ce qui précède est l'alaphabet phonétique de l'Otan. Mais tout ce qui touche à la sécurité l'utilise. Police, pompiers, forces armées, protection civile…

C'est un moyen simple et efficace pour éviter les bévues dues aux mauvaises compréhensions. Apprenez-le par cœur, vous y arriverez très vite. Et si vous ne l'utilisez jamais lors d'une mission, vous trouverez bien un jour un moyen de frimer avec.

Si votre cible a un emploi du temps régulier, une technique qui permet à l'agent de ne pas se faire détecter est la segmentation de la mission sur plusieurs jours. Le premier jour, vous suivez la cible sur une distance plus ou moins courte. Le deuxième jour, vous reprenez la filature à partir du point d'arrêt de la veille. C'est une technique plutôt utilisée par la police ou les services de renseignement quand il s'agit, par exemple, d'identifier le domicile de la cible.

2. La planque

La planque se distingue de la filature par le fait qu'ici, nous sommes dans le cadre d'une observation statique. Elle peut se pratiquer en milieu rubain ou non-urbain et nous verrons que ce sera tout à fait différent. Mais quel que soit l'endoit, vous ne savez pas combien de temps ça va durer. Prévoyez donc de quoi boire et manger et pour les plus motivés, des langes.

En milieu urbain

Normalement la foule ou la circulation vous protège. Si vous êtes dans une voiture, essayez de vous garer de façon à

observer via votre rétroviseur, c'est beaucoup plus discret. C'est très dur car votre attention ne peut pas chuter une seonde. Une seconde, c'est le temps qu'une porte s'ouvre ou qu'un bus passe. Là aussi, nous avons une belle différence avec les films : raconter sa vie à son partenaire en buvant des coups, c'est sympa, mais ça n'est pas la réalité. Ici, vous observez et c'est tout. Longtemps.

Si vous avez la chance de pouvoir planquer dans un bar, c'est parfait. Personne ne vous demandera rien tant que vous consommez. A ce propos, vous payez votre verre quand vous le recevez. Pas chouette si vous devez fouiller le fond de vos poches au moment où votre cible sort de chez elle, ou pire, attendre le change parce que vous n'avez qu'un billet de 50 euros.

Je ne parle pas du cas très cinématographique où vous avez loué l'appart en face de votre cible pour l'observer H24, parce que désolé, ça n'existe pas dans le privé.

En milieu rural ou péri-urbain

Planquer à la campagne ou dans un lotissement est drôlement compliqué. Si vous restez dans votre voiture, vous serez repéré. Contrairement à ce qui se passerait en ville, si vous êtes repéré en milieu rural ou dans un lotissement, quelqu'un viendra très vite vous demander ce que vous faites là ou appelera la police. Vous ne commettez pas de délit, mais la planque sera terminée.

Si vous n'avez pas d'autre option, prévoyez au minimum une histoire qui justifie votre présence. Agent immobilier en repérage, futur habitant du quartier…

Si la mission le permet, l'observation à distance est une bonne option. Equipé d'un monoculaire puissant avec vision nocturne, vous pouvez rester en planque durant de longues heures, sans rien perdre des activités de votre cible. Pour ne rien manquer et si vous avez un créneau pour les installer, l'utilisation de caméras espion vous sera d'un grand secour.

La meilleure option ici est le sous-marin, c'est-à-dire un véhicule déguisé à des fins de renseignement. Une camionnette avec un logo de plombier ou d'électricien est très bien. Avec un numéro de téléphone auquel vous répondez si un voisin vérifie. Si vous avez la chance de pouvoir planquer depuis la place de l'église, vous devriez avoir la paix à condition que l'entourage ne puisse pas identifier que vous êtes dans le véhicule. Sinon, garez-vous de façon à faire croire aux gens du coin que vous réalisez des travaux chez un voisin. Portez des vêtements d'ouvrier ou de technicien, avec une casquette car c'est exactement le profil auxquel personne ne prète attention. Votre tenue ne sera ni trop neuve ni trop propre.

Si vous ne savez pas combien de temps va durer le travail, prévoyez aussi des vêtements de rechange. Bonne nuit.

XIII. Gérer son réseau d'informateurs de façon totalement anonyme

Voilà c'est fait, vous avez votre réseau d'informateurs. Ils travaillent dans des ministères, des banques ou des entreprises de télécommunication. Comme vous n'oeuvrez pas contre les intérêts d'un pays, vous êtes dans le renseignement privé rappellons-le, le risque est faible de vous retrouver avec un groupe d'agents du Mossad planqués dans votre jardin. Cependant, vous êtes prudent et je vous en félicite.

Vous avez forcément rencontré à diverses reprises les membres de votre réseau, mais par discrétion, vous souhaitez pouvoir communiquer avec eux en tout anonymat. Surtout, vous voulez un moyen sûr de recevoir leurs informations. Avant Internet, il fallait utiliser deux moyens fort dangereux. La boite aux lettres morte ou l'échange physique. La boite aux lettres morte est n'importe quoi dans l'espace public où un agent peut laisser un document ou un message. Une marque prévient que la livraison a été effectuée. Cette marque peut être à proximité de la boite aux lettres ou dans n'importe quelle partie de la ville. Les dispositifs de signalisation peuvent comprendre une marque à la craie sur un mur, un morceau de chewing-gum sur un lampadaire ou un journal laissé sur un banc de parc. Le signal peut également être émis de l'intérieur de la maison de l'agent, par exemple en suspendant une serviette de couleur particulière sur un balcon ou en plaçant une plante en pot sur un rebord de fenêtre où elle est visible par tous les habitants de la rue. Bien que la méthode de la livraison directe soit utile pour empêcher la capture instantanée d'un

couple d'agents ou d'un réseau entier, elle n'est pas à toute épreuve. Si l'un des agents est compromis, il peut révéler l'emplacement et le signal de ce point de chute spécifique. La police peut alors utiliser le signal tout en gardant le lieu sous surveillance, et peut capturer l'autre agent. Un autre inconvénient est qu'un opérateur va transporter sur lui durant un certain temps quelque chose qui peut lui nuire. Ce sera pareil quand vous viendrez récupérer le matériel. Vous l'avez sur vous. Enfin, si votre informateur habite à 800 kms, ça n'est pas très pratique.

La technique de l'échange suppose que deux agents se croisent dans l'espace public (rue, magasin, toilettes…) et que l'un donne quelque chose à l'autre. Outre le côté stressant, les inconvénients sont les mêmes qu'avec la boite aux lettres morte.

C'est pourquoi au départ de votre mission, vous avez tout simplement créé un compte sur une messagerie gratuite. Comme vous avez du donner une adresse email pour la confirmation de la création de l'adresse, vous avez pris soin de le faire avec une adresse email jetable. Vous avez installé un VPN pour qu'on ne puisse pas localiser votre adresse IP, vous n'utilisez jamais Google car vous savez que tout est enregistré et à la place, vous travaillez avec Duckduckgo. Vous effacez toute trace sur votre machine avec un excellent outil gratuit, ccleaner https://www.ccleaner.com/ mais vous prenez quand même l'option payante car elle vous permet un bien plus beau nettoyage en profondeur.

Lorsque votre informateur est recruté, vous lui demandez de mémoriser l'adresse email et le code d'accès. Vous lui donnez les consignes de sécurité :

- Ne jamais utiliser l'ordinateur du bureau car tout est enregistré sur le serveur de la boite.
- Utiliser un VPN et ccleaner.
- Se rendre sur le net exclusivement via duckduckgo.

Vous n'utilisez jamais votre nom, ni celui de l'opérateur. Vous pouvez choisir les noms que vous voulez, mais aucun qui vous relie à lui. A une lointaine époque, j'avais une informatrice baptisée « Angelina». Pourquoi ? Parce qu'elle était le sosie de l'actrice américaine Angelina Jolie.

Pour payer votre informateur, ce sera via un compte offshore si on parle de gros montants. S'il s'agit de sommes de quelques centaines ou milliers d'euros, vous utilisez un système de boite aux lettres morte. C'est peu dangereux car si vous ou lui êtes pris, vous avez une histoire toute prête qui justifie que vous soyez en possession de cette somme. S'il s'agit de 100.000. euros, ne perdez pas votre temps à inventer une histoire, vous êtes pris.

Chaque fois que votre informateur souhaite vous communiquer des informations, il se connecte à la boite mail, rédige son message avec son nom de code en en-tête, avec un attachement si nécessaire et enregistre le tout dans les brouillons. Aucun message n'est envoyé. Pas de circulation de l'information. Quand vous vous connectez à votre tour sur la messagerie, vous accédez au message et ensuite vous l'effacez. La boite est vide. Vous faites tourner

ccleaner. Bien entendu, il y a toujours un risque si vous devez télécharger des données. Au minimum, faites le en téléchargeant sur une clé USB cryptée. Une façon encore plus discrète de procéder est de se créer un compte sur un site de jeux ou de rencontres. En tout cas un site où il est possible d'écrire un message puis de l'enregistrer sans l'envoyer. C'est très bien mais il est rare qu'il soit possible de sauvegarder des pièces en attachement.

Le risque ici est surtout lié à la routine. Vous savez que votre vie n'est pas en jeu. Les délits commis ne vous enverront pas 20 ans derrière les barreaux. J'ai connu des gens dans la sécurité privée qui allaient régulièrement se faire un resto avec leurs sources et qui juste avant le dessert, sortaient une petite enveloppe. Ils se sont fait prendre et ont passé quelques semaines ou quelques mois en prison. Si vous êtes vraiment prudent, ça ne se produira pas. Mais ce qui est compliqué, c'est de contrôler le niveau de vigilance de vos opérateurs. La sécurité, c'est bien, mais ça fait perdre du temps. Comme rien ne se passe jamais, on a tendance à se relacher. Comme souvent, le facteur humain sera notre perte.

XIV. Conclusions

Il y a quelques années, j'ai écrit un livre qui portait un titre peu ambigu : « comment pourrir la vie de son patron ». Il s'agissait de recettes de sales coups. Certaines étaient simplement gentiment potaches. D'autres, d'une intensité à ruiner la vie de votre boss. Beaucoup de gens me demandaient si je ne craignais pas que des gens malintentionnés utilisent le contenu du livre pour nuire à leur patron. A chaque fois, je posais la même question : « et vous, vous le feriez ? ». A chaque fois, la personne me répondait que elle, non, mais que les autres, oui peut être. Il est bien connu que le mal, ce sont les autres. J'avais écrit ce bouquin parce que j'en avais marre d'entendre les gens pleurnicher dans les entreprises. Pleurnicher à propos du fait que le patron ou le manager avait tous les pouvoirs et eux, aucun. Quand vous savez que si vous le souhaitez, vous tenez l'existence même de votre patron entre vos mains, il est beaucoup plus difficile de se positionner en tant que victime professionnelle.

« Le renseignement offensif » peut être vu exactement de la même manière. Un livre sur le pouvoir que n'importe quel anonyme détient s'il le souhaite. Vous savez maintenant que la vie privée est une histoire du passé, que vous pouvez obtenir n'importe quelle information sans pour autant appartenir à un organisme de renseignement d'état. Et que si vous le voulez, vous pouvez nuire grandement à n'importe quelle entreprise. Même si aucun chapitre n'est explicitement consacré à la destruction de quoi que ce soit, la lecture avisée de nombreux chapitres vous donne la puissance d'une arme de destruction massive. La vérité,

c’est que j’espère que personne ne nuira à personne et que chacun puisse y trouver ce qu’il est venu chercher.

A un autre niveau, ce livre se veut un livre entièrement consacré à la sécurité. Personne n’aime prendre la place de la victime. Raison pour laquelle, les livres consacrés à la sécurité ne rencontrent pas un vrai succès de masse. Ici, vous êtes dans la peau de l’attaquant. C’est bien plus rigolo et tout aussi instructif. Quand vous voyez ce qu’il est possible de faire avec peu de moyens, vous pouvez commencer à réfléchir à comment vous protéger.

Enfin, l’authentique finalité de ce livre n’est ni la sécurité ni une ode au pouvoir. C’est un manuel pratique qui vise à vous enseigner comment obtenir du renseignement sur les entreprises et les décideurs. Le reste n’est à mes yeux que secondaire.

Je vous suggère de travailler avec la version papier et la version électronique. Il y a beaucoup de liens cliquables et avec la version papier, vous devrez retaper manuellement les liens et c’est plutôt ennuyeux à faire.

Par anticipation, mea culpa pour les liens morts sur lesquels vous allez probablement tomber. On meurt jeune sur le net et beaucoup de choses disparaissent très vite. Si vous tomber sur une erreur, une incohérence ou sur un lien disparu, faites-le moi savoir et je pourrai continuellement tenir ce manuel à jour. Idem si vous avez vent d’une technique ou d’un outil qui mériterait d’être connu de tous.

Pour me joindre,

philippedylewski@gmail.com


Philippe Dylewski
LE RENSEIGNEMENT OFFENSIF
300 techniques, outils et astuces pour tout savoir sur tout le monde, dans les entreprises et ailleurs
Deuxième édition mise à jour 2021
DÉCONFIDENTIALISÉ
AGAKURE


LE RENSEIGNEMENT
OFFENSIF
Philippe Dylewski
Ce livre est un condensé de trucs, outils et techniques qui permettent de tout savoir sur tout le monde, dans le monde des entreprises et ailleurs. Ce manuel résolument pratique vous apprendra à trouver l'information en utilisant les secrets du Google Hacking et du dark web. Vous pourrez localiser une personne grâce à une simple photo, une adresse email ou un numéro de téléphone. Vous connaîtrez tout de la situation et des projets de vos concurrents et partenaires.
Philippe Dylewski a une formation de psychologue. Il a dirigé un cabinet de recrutement pendant 15 ans avant de devenir détective privé, puis spécialiste du renseignement d'affaires, notamment dans le cadre de fusions ou d'acquisitions. Il vit aujourd'hui en Thaïlande et coordonne les activités d'un groupe spécialisé dans la recherche de personnes disparues à travers le monde. Il a été publié chez l'Express, fayard, les Editions du Nouveau Monde et l'Institut Pandore.
ISBN : 979-10-96819-01-0
EAN : 9791096819010