Formation OSINT VOL.2

Sommaire

INTRODUCTION

LC
@DalilBoubakeur

La première formation a été l'occasion pour moi de vous introduire au monde de l'OSINT, vous avez vu sur les réseaux sociaux, et en particulier sur Twitter, comment avec des connaissances et des maîtrises, nous pouvons remonter des données personnelles sur des individus, les localiser ainsi que les identifier.

Cette formation entre en profondeur dans cette approche, apporte de nouveaux outils, de nouvelles méthodes de recherches, ainsi que des éléments pour cacher sa propre identité sur Internet.

Je vous remercie par avance pour m'avoir fait confiance, et je vous souhaite une excellente lecture.

LC

Glossaire

Ces mots reviendront à plusieurs reprises dans la formation, il est important que vous puissiez les connaître en amont.

01. SOCMINT

Social media intelligence, ensemble de solutions pour surveiller des activités liées aux Réseaux Sociaux.

02. OSINT

Open Source Intelligence, renseignements obtenus par des sources publiques.

03. REGEX

Expressions régulières, très utilisés dans le monde de l'informatique.

04. TOR

The Onion Router, réseau informatique superposé mondial et décentralisé.

05. VPN

Virtual Private Network, tunnel sécurisé entre deux équipements ou sites.

06. PsyOps

Opération psychologique

07. OpSec

Securité opérationnelle

08. Live OS

Système d'exploitation non-persistant

09. EFF

Electronique Frontier Foundation

10. API

Interface de programmation, permet de faire un appel extérieur pour communiquer une application

1 - RAPPEL DE LA METHODOLOGIE

Une méthodologie ? Oui une méthodologie, car, l'OSINT n'est pas seulement un ensemble d'outils, mais bien une méthodologie qu'il va falloir appliquer avec rigueur pour toutes vos investigations afin de ne pas se perdre dans un amas d'informations.

Cette dernière se déroule en plusieurs étapes : **Définition des recherches – Collecte & Analyse, Vérification & Croisement de données - Mise en évidence.**

En complément à cette méthodologie, l'utilisation d'outils va permettre de faciliter considérablement votre travail de collecte et parfois même d'analyse. Car si ces derniers sont bien évidemment nécessaires pour trouver de l'information, aucun outil n'est indispensable et ne saurait fonctionner correctement sans une compréhension du fonctionnement de ce dernier et sans un traitement humain, du moins pour l'instant.

Je vais vous donner un exemple basique : Google.

En effet, Google est un moteur de recherche très puissant qui va permettre de lancer des requêtes pour obtenir de nombreuses informations. Mais il existe une énorme différence entre le novice qui se contente de taper des mots clés en espérant que l'algorithme trouve exactement ce dont il a besoin et l'utilisateur qui maîtrise l'ensemble des expressions régulières de Google afin de se concentrer sur un périmètre beaucoup plus réduit et donc de facto trouver des informations beaucoup plus pertinentes. Cet aspect est fondamental, que ce soit en amont pour définir le cadre de recherche, pendant pour la collecte, ou après pour l'analyse & le croisement de données.

1.1.1 Définition des recherches

Première étape de l'OSINT : la définition des recherches. Il s'agit donc, avant de se lancer, de clairement définir ce qui est recherché : s'agit-il d'évaluer la réputation ou fiabilité d'un vendeur ? D'obtenir des coordonnées d'un particulier ou d'une entreprise ?

Les domaines de recherche sont extrêmement nombreux et ne réclameront pas la focalisation sur le même environnement et sur les mêmes sources d'informations. Ainsi, dans certains cas, il sera plus pertinent de s'intéresser aux réseaux sociaux, tandis que d'autres dossiers nécessiteront d'interroger des documents officiels par le biais de bases de données spécialisées (Immatriculation de véhicule, Registre de commerce etc…).

1.1.2 Collecte & Analyse

Une fois l'objet des recherches défini, la phase de collecte d'information et d'analyse va pouvoir commencer. Afin d'éviter de prendre une mauvaise direction dès le début, il va falloir se baser sur des informations sûres et/ou les éléments les plus caractéristiques pour lancer ses recherches.

« Chercher, Trouver, Analyser, Répéter. » L'OSINT, c'est par définition l'accumulation d'informations et leur combinaison pour en extraire de nouvelles, jusqu'à obtenir ce que l'objet de notre quête.

1.1.3 Vérification & Croisement des données

Pour se démarquer et réaliser de bonnes investigations, cette étape est primordiale. Elle va consister à prendre l'ensemble des informations qui ont été préanalysées par vos soins et vérifier que ces dernières soient pertinentes en les croisant pour obtenir des preuves tangibles.

Le croisement de données est également utile pour trouver d'autres informations. Un bon investigateur va avoir la capacité à élaborer un chemin de collecte d'informations lui permettant de trouver ce qu'il cherche. À partir d'une information A de base, il n'est parfois pas possible d'accéder à une information C. En revanche, A peut mener à une information B, puis B peut mener à C.

1.1.4 Mise en évidence

Cette étape est nécessaire pour mettre en évidence l'ensemble de vos preuves afin d'établir un ordre chronologique, le profil d'une personne ou la hiérarchie d'une organisation par exemple.

Au final, la qualité d'un bon chercheur va résider dans les connaissances de la méthodologie, de la multitude d'outils via une veille technologique pour parvenir aux collectes, dans sa capacité à tirer profit au maximum des informations dont il dispose et à établir des connexions entre elles pour en recueillir de nouvelles. Bien évidemment, plus un chercheur maîtrise d'outils, plus il aura de chance de trouver ce qu'il cherche. Or, votre cerveau sera toujours votre meilleur atout alors utilisez-le.

Voici un site extrêmement utile pour trouver les outils adéquats en plus de ceux renseignés dans la formation : https://osintframework.com/

2 - OPSEC

2.1 Principe de l'OpSec

Définition d'une OpSec :

Selon Wikipédia, OpSec (pour « Operations Security », en français Sécurité opérationnelle) est une méthode utile pour se prémunir des risques que peut courir une structure si ses informations sensibles étaient acquises par un adversaire à cette structure.

C'est un processus qui va identifier des informations critiques afin de déterminer si des actions amicales peuvent être observées par le renseignement ennemi, déterminer si les informations obtenues par l'adversaire pourraient être interprétées comme leur étant utiles pour ensuite exécuter des mesures choisies qui éliminent ou réduisent l'exploitation par l'adversaire d'informations critiques amicales.

Dans un sens plus général, une OpSec consiste en un ensemble de processus de protection des données individuelles qui pourraient être regroupées pour donner une « image plus grande » (appelée agrégation) d'une organisation particulière. Elle va être la protection des informations critiques jugées essentielles aux missions par les commandants militaires, les hauts responsables, la direction ou tout autre organe décisionnel.

Le processus aboutit au développement de contre-mesures qui comprennent des mesures techniques et non techniques, telles que l'utilisation d'un logiciel de chiffrement de messagerie, en prenant des précautions contre l'espionnage, en prêtant une attention particulière aux photos prises (comme des éléments en arrière-plan **#GEOINT**), ou le fait de ne pas parler ouvertement sur les sites de médias sociaux d'informations critiques de l'activité ou de l'organisation d'une unité.

L'OpSec au niveau « Cyber » va être une notion très personnelle, car elle va dépendre de toute l'expérience et de la maturité dans la compréhension des différents acteurs dans le Web.

NB : le terme « Operations Security » fut formalisé par l'armée américaine pendant la guerre du Viêt Nam.

Voici les 5 grandes étapes afin d'établir une OPSEC :

- Identifier l'information critique à protéger ;
- Analyser les menaces ;
- Analyser les vulnérabilités ;
- Évaluer les risques ;
- Appliquer des contre-mesures.

Cas pratique :

Vous êtes un pirate informatique affilié au gouvernement vénézuélien qui vend des infos sensibles du gouvernement US, le tout en étant basé au Brésil. En amont, vous allez identifier l'information critique à protéger :

- Identité personnelle
- Adresse IP
- Installation informatique
- Géolocalisation

Vous allez ensuite analyser les menaces. Dans cet exemple celles-ci seront :

- Gouvernement US (et ses alliés exemple : 5 EYES, OTAN…)
- Gouvernement brésilien
- Potentiels autres acteurs sur votre marché

Maintenant vous allez analyser les vulnérabilités :

- Leak d'informations sensibles
- Intégrité de vos installations informatique (multiples vecteurs d'attaques)
- Retraçage de vos activités
- Probabilité de tomber sur un honeypot durant vos actions pouvant vous compromettre.

Evaluons maintenant les risques :

Dans ce cas les risques sont tous élevés. Personnellement, je rédige une matrice Excel en classant mes risques par trois degrés de niveau (Elevé, Moyen, Faible), mais chacun sa façon de faire de se coté là.

Une fois l'ensemble des processus effectués, il va falloir appliquer des contre-mesures :

- Pour le leak d'informations sensibles ainsi que le retraçage de vos activités, il va falloir contrôler et faire extrêmement attention à toutes les informations que vous allez être amené à divulguer sur le Web, que ce soit vos connaissances ou non.
- Concernant l'intégrité de vos installations informatiques, je vous conseille de vous renseigner d'un point de vue géopolitique et de faire un choix au sujet de ce contre quoi vous voulez vraiment vous protéger. Ce faisant, vous pourrez également déterminer ce que vous exposez suite à ce choix.
    - Exemple : une personne obtenant un accès TOR a toutes les chances de se faire repérer par les US qui contrôlent beaucoup de nœuds de sortie Tor... (d'où le contrôle de nœuds, mais nous verrons cela par la suite). Par contre héberger cet accès ou passer par un pays ennemi des US vous expose aussi à une saisie du gouvernement local si jamais ils n'aiment pas vos activités (typiquement, ils pourraient vous faire pression en vous indiquant qu'ils savent ce que vous faites). Pareil pour l'utilisation d'un VPN. Celui-ci va vous protéger contre l'interception de la connexion Internet, mais cela va vous exposer à l'interception (et l'injection) de celui de qui vous allez obtenir votre accès VPN. Vous allez aussi devoir mettre en place beaucoup de mesures cryptographiques afin de contrôler l'accès physique et distant de votre environnement de travail.
- Pour le retraçage des activités et pour éviter de tomber sur des honeypots, il va falloir créer plusieurs identités avec un background convaincant afin de brouiller les pistes.

2.2 Sécurité de l'environnement de travail

2.2.1 Sécurité Physique

Une sécurité physique est essentielle, raison pour laquelle c'est la première étape pour le plan de sécurité de votre équipement. Je vous conseille de suivre les recommandations de l'ANSSI (par exemple si vous avez un pc portable, collez un autocollant sur le dessous de votre pc afin de savoir si ce dernier a été démonté ou non, désactivez aussi les ports USB si nécessaire, etc…).

2.2.2 Sécurité du BIOS

Au sujet de la sécurité du BIOS, qui est un ensemble de fonctions contenues dans la mémoire morte (ROM) de la carte mère d'un ordinateur lui permettant d'effectuer des opérations de base lors de sa mise sous tension (Amorçage de l'OS par exemple), je vous conseille de mettre un mot de passe afin qu'un attaquant ne puisse pas amorcer un autre OS sur le poste pour effectuer des manipulations sur vos données ou bien installer un rootkit ou autre menace.

2.2.3 OS Hardening

L'OS Hardening ou durcissement de Système d'Exploitation va consister à réduire la surface d'attaque dont disposent les agresseurs. Il est basé sur le principe du « moindre privilège » afin que votre OS ne fasse que ce que vous faites normalement et rien de plus.

Le durcissement fait partie intégrante de la sécurité de l'information et comprend les principes de dissuasion, de refus et de détection (le durcissement couvre les trois).

Exemple basé sur Windows 10 :

Installation sécurisée

Il est fortement recommandé d'installer Windows 10 sur un système récent, car les systèmes précédemment utilisés peuvent contenir des logiciels malveillants, des logiciels espions et les systèmes préinstallés des constructeurs peuvent contenir une quantité absurde de logiciels espions. Créez ou trouvez un support d'installation approprié pour votre système Windows 10 (une clé USB de confiance, de préférence). Veillez à éteindre le système Wifi de votre système et à débrancher sa connexion Ethernet lors de l'installation.

Nettoyer les programmes indésirables

Même dans les nouvelles installations de Windows 10, un système a probablement des programmes inutiles installés. Ces programmes élargissent la surface d'attaque et deviennent des points d'entrée potentiels pour les attaquants. Les programmes installés doivent être examinés, puis les programmes inutiles supprimés. Vérifiez que tous les programmes installés sont légitimes et ne sont pas des logiciels piratés, qui pourraient être remplis de boursouflures et de logiciels malveillants.

Chiffrement

Ne tournons pas autour du pot : les disques durs doivent être chiffrés. Heureusement, Windows 10 est livré avec BitLocker comme solution de chiffrement intégrée, dont le processus est facile. Il faut toutefois noter que la puce Trusted Platform Module (TPM) doit être activée afin de

pouvoir chiffrer avec BitLocker, mais les éditions ultérieures de Windows 10 sont de facto livrées avec le TPM activé par défaut. Le démarrage sécurisé doit être utilisé en conjonction avec le chiffrement, puisqu'il reliera le disque dur au matériel du système et garantira que seul le micrologiciel de confiance de Microsoft est utilisé au démarrage.

Mises à jour, correctifs et service packs

Assurez-vous que le système Windows 10 est au point en termes de mises à jour, correctifs et service packs. Un système Windows 10 qui n'est pas au à jour est une cible plus facile pour les attaquants.

Guards

Windows 10 dispose de plusieurs solutions de sécurité intégrées pour différents aspects du système d'exploitation qui utilisent "Guard" comme nom de fonction.

Se débarrasser des services inutiles

Les systèmes Windows 10 contiennent de nombreux services que les organisations ne veulent pas ou n'ont pas besoin de faire fonctionner, raisons pour lesquelles le système doit être vérifié à la fois pour les services indésirables, mais également pour ceux qui sont préinstallés (OOBE).

Windows Defender

Magic Quadran Endpoint de Gartner 2019

En effet Microsoft a intégré dans Windows 10 une solution antivirus (AV) gratuite qui ne présente pas de « faiblesses majeures » et qui ne fonctionne pas mal, contrairement à la plupart des solutions AV gratuites. Windows Defender doit être activé par défaut ; pour le vérifier, ouvrez le tableau de bord de Windows Defender.

Politique de groupe

Cette technique est trop vaste pour en donner une lecture exhaustive, car les organisations ont leurs propres besoins spécifiques et Windows dispose d'une énorme quantité de politiques de groupe. Les organisations dotées d'un département informatique disposent normalement de paramètres de base de politique de groupe qui sont configurés pour chaque nouvelle machine Windows 10 embarquée. Un système Windows 10 doit se conformer à cette politique de groupe de base dès le premier démarrage. Les mots de passe sont un des paramètres de la politique de groupe qui est communément universel dans les organisations. Une politique de groupe de mots de passe devrait imposer des mots de passe complexes et définir un intervalle de réinitialisation des mots de passe.

Protection contre les ransomwares

Windows Defender offre une protection contre les logiciels de rançon, mais elle n'est pas activée par défaut. Pendant le processus de durcissement, regardez dans Virus & Threat Protection → Ransomware protection → Manage ransomware protection. Assurez-vous que l'accès aux dossiers contrôlés est activé. Gardez à l'esprit que cela empêchera les applications de créer des fichiers dans le dossier des documents.

Authentification sécurisée

L'authentification doit être renforcée, car elle peut constituer une surface d'attaque flagrante. Le meilleur moyen d'y parvenir est de mettre en place une authentification multifactorielle. L'un des facteurs peut être un mot de passe complexe, l'autre étant soit un code PIN, un mot de passe gestuel, biométrique ou une image.

2.3 Gestionnaire de mot de passe

Un gestionnaire de mots de passe est un type de logiciel ou de service en ligne qui va vous permettre de gérer l'ensemble de vos mots de passe, soit en centralisant l'ensemble de ses identifiants et mots de passe dans une base de données (portefeuille), soit en les calculant à la demande. Le gestionnaire de mots de passe est protégé par un mot de passe unique, afin de n'en avoir plus qu'un seul à retenir.

L'utilisateur, ainsi affranchi de la contrainte de se souvenir de ses différents mots de passe, peut aussi se permettre d'en choisir de plus compliqués (et donc de plus robustes), et d'avoir un mot de passe différent pour chaque compte ou chaque document (de sorte que si l'un des mots de passe est intercepté, les autres comptes ou documents ne sont pas rendus vulnérables).

Pour cela j'utilise le gestionnaire Keepass XC car il assure aussi une fonction de 2FA.

2.4 Checksum

Une somme de contrôle (checksum en anglais) est une courte séquence de données numériques calculée à partir d'un bloc de données plus important (par exemple un fichier ou un message) permettant de vérifier que l'intégrité de ce bloc a été préservée lors d'une opération de copie, stockage ou transmission. On parle aussi parfois d'empreinte numérique

(hash). Pour l'utilisateur final, les sommes de contrôle se présentent typiquement sous la forme de nombres au format hexadécimal.

Exemple sur le site de GIMP :

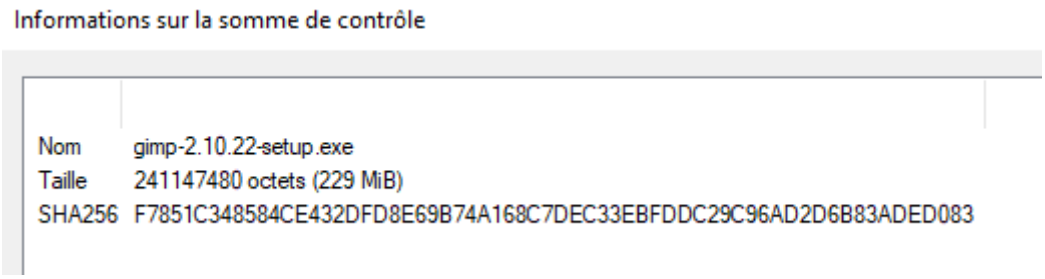
Hash Sum

The SHA256 hash sum for `gimp-2.10.22-setup.exe` is:

`f7851c348584ce432dfd8e69b74a168c7dec33ebfddc29c96ad2d6b83aded083`

Pour vérifier l'intégrité du téléchargement du .EXE, vous allez vérifier que le Hash en SHA 256 est le même que celui annoncé sur le site.

Sous Windows :



Sous linux en CLI :

```
sha256sum nom_du_fichier
```

2.5 TOR

2.5.1 Qu'est-ce que TOR ?

Tor est un réseau informatique superposé mondial et décentralisé. Il se compose d'un certain nombre de serveurs, appelés nœuds TOR et dont la liste est publique. Ce réseau va permettre d'anonymiser l'origine de connexions TCP. TOR peut servir à anonymiser la source d'une session de navigation Web ou de messagerie instantanée. Il est utilisé pour se protéger contre une certaine forme de surveillance sur Internet. Ce réseau est aussi un outil de contournement de la censure car il va permettre aux personnes l'utilisant d'accéder à des sites, contenus ou services bloqués dans certaines zones du monde.

Ce réseau est aussi un outil de contournement de la censure, car il permet aux personnes l'utilisant d'accéder à des sites, contenus ou services bloqués dans certaines zones du monde.

Tor fait circuler le trafic des personnes utilisatrices via une série de relais. Ce procédé permet **théoriquement** de ne pas être suivi par les sites web consultés, d'accéder à des services, contenus ou sites bloqués par un FAI. Il est aussi possible pour chaque personne utilisatrice de publier des contenus via les services « onion » de Tor, sans révéler la position de ces services.

Ces avantages peuvent être utiles pour chaque personne utilisatrice qui souhaite maîtriser ses traces laissées en ligne. Ils sont notamment mis en œuvre dans les échanges entre personnes lanceuses d'alerte, journalistes, avocats, dissidents politiques, représentants d'organisations non gouvernementales, ou pour échanger en maîtrisant la sécurité de leurs données, de leur connexion, de leurs destinataires et de leur position. Il peut aussi servir à des personnes ou organisations malveillantes en permettant un possible anonymat.

Néanmoins des précautions sont à prendre, car Tor n'assure pas un anonymat absolu.

2.5.2 Installation

Voici des liens de tutoriels écrits par l'EFF sur comment installer TOR sous Windows & Linux.

Windows: https://ssd.eff.org/fr/module/guide-pratique-utiliser-tor-pour-windows

Linux : https://ssd.eff.org/fr/module/guide-pratique-utiliser-tor-pour-linux

2.5.3 Tor Bridge & Pluggable Transport

Si vous êtes dans un endroit où les FAI avec la complicité du gouvernement interdisent l'usage de Tor, les ponts peuvent vous aider à contourner cet usage. Les ponts Tor sont des points d'entrée alternatifs dans le réseau Tor qui ne sont pas listés publiquement. Utiliser un pont rend plus difficile, mais pas impossible, pour votre Fournisseur d'Accès à Internet de savoir que vous utilisez Tor.

Voici le lien de la fondation Tor sur comment obtenir cette liste de ponts : https://tb-manual.torproject.org/bridges/

2.5.4 Contrôle des nœuds de sortie

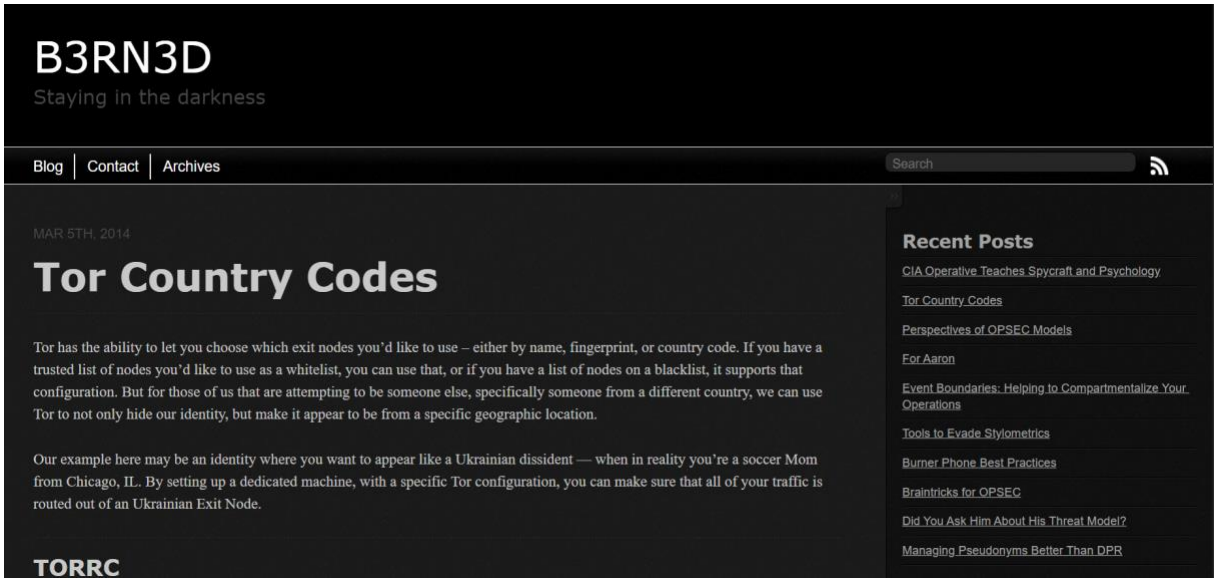
Tor vous permet de choisir les nœuds de sortie que vous souhaitez utiliser soit par nom, soit par empreinte numérique, soit par code pays. Si vous avez une liste de nœuds de confiance que vous souhaitez utiliser comme liste blanche, vous pouvez l'utiliser, ou si vous avez une liste de nœuds sur une liste noire, il supporte cette configuration. Mais pour ceux d'entre nous qui tentent d'être quelqu'un d'autre, en particulier quelqu'un d'un pays différent, nous pouvons

utiliser Tor non seulement pour cacher notre identité, mais aussi pour la faire apparaître comme provenant d'un lieu géographique spécifique.

Pour cela, il va falloir modifier le fichier torrc :

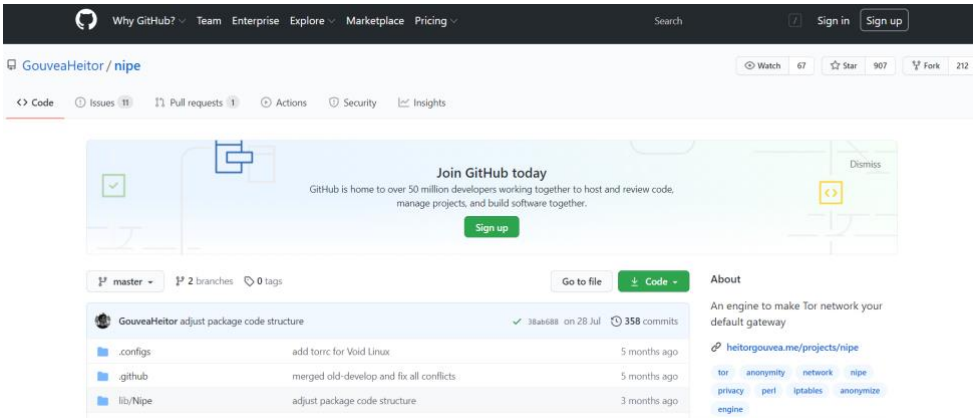
Sous Windows ou Linux, le fichier torrc se trouve dans le répertoire Tor Browser au chemin suivant **TorBrowser/Data/Tor**.

Voici un lien montrant plusieurs exemples de configurations :
https://b3rn3d.herokuapp.com/blog/2014/03/05/tor-country-codes



2.5.5 Router tout son trafic par TOR sous Linux

Voici un script qui fonctionne sous Linux et qui va vous permettre de faire passer l'ensemble de votre trafic par Tor, pour rappel la distribution Tails le fait aussi nativement : https://github.com/GouveaHeitor/nipe



2.5.6 Faiblesses de TOR

Il faut savoir que ce projet est en partie financé par le gouvernement américain, car c'est aussi un outil qui sert à masquer le trafic des agents du renseignement américain comme l'explique Dingledine, cofondateur du projet.

Aussi, n'importe qui peut gérer un nœud Tor : un hacker, un espion ou une agence gouvernementale, lorsqu'on découvre le principe du réseau, sa nature axée autour de la décentralisation semble être un gros point positif. Mais bien qu'il y ait des avantages à la décentralisation, celle-ci amène aussi son lot de problèmes… Le principal étant que n'importe qui peut opérer les nœuds du réseau Tor qui vont servir à router le trafic. Il est arrivé plusieurs fois que des personnes mal intentionnées aient mis en place un nœud Tor pour récupérer des informations sur ses utilisateurs. Il y a beaucoup de preuves aussi sur une potentielle coopération entre les développeurs de TOR et les agences gouvernementales américaines, mais je vous laisse faire vos recherches par vous-même.

2.5.7 Mesures d'atténuation pour réduire les risques

Pour conclure TOR est un bon moyen de contourner les censures et d'assurer un niveau de confidentialité, mais il va falloir mettre en place d'autres mesures pour se garantir un possible anonymat. L'utilisation d'un VPN est recommandée en complément, la mise en place d'un firewall (PFsense, Iptable etc.) ainsi que des mesures sur le navigateur Web que nous allons voir par la suite.

2.6 VPN

2.6.1 Qu'est-ce qu'un VPN ?

En informatique, un réseau privé virtuel ou réseau virtuel, plus communément abrégé en VPN (de l'anglais : Virtual Private Network), est un système permettant de créer un tunnel direct entre des ordinateurs distants, qui isole leurs échanges du reste du trafic se déroulant sur des réseaux de télécommunication publics.

2.6.2 Protocoles

2.6.2.1 SSL/TLS

Le terme « VPN SSL/TLS » désigne une catégorie de produits en évolution rapide qui incluent une variété de technologies.

Les VPN SSL utilisent une méthodologie différente pour transférer des données privées sur Internet. Plutôt que de s'appuyer sur les paramètres réseau et la sécurité des points de terminaison, le VPN SSL utilise le protocole HTTPS, qui est disponible dans tous les navigateurs Web standard.

Les VPN SSL utilisent une méthodologie différente pour transférer des données privées sur Internet. Plutôt que de s'appuyer sur les paramètres réseau et la sécurité des points de terminaison, le VPN SSL utilise le protocole HTTPS, qui est disponible dans tous les navigateurs Web standard et qui est un mécanisme de transmission sécurisé qui ne nécessite pas de logiciel supplémentaire. Avec le VPN SSL, la communication entre l'utilisateur mobile et les ressources back-end s'effectue via la connexion réseau au niveau de la couche application, par opposition à une connexion VPN IPSec ouverte au niveau de la couche réseau.

La technologie VPN SSL est utilisée dans divers types de connexions. Cet avantage permet l'utilisation du VPN SSL pour prendre en charge les applications client-serveur, dans les situations où une connexion réseau à tunnel complet est créée. Cette transmission dynamique facilite l'installation et la configuration du logiciel de chaque client.

2.6.2.2 IP Sec

Une connexion VPN IPSec peut offrir aux entreprises un moyen simple et économique d'acheminer des paquets de données entre des points. Il offre une connectivité et une résilience solides pour répondre aux besoins des environnements réseau les plus exigeants. Cette alternative à la location d'une ligne dédiée permet aux entreprises de tirer parti de l'infrastructure Internet pour étendre rapidement leur réseau à des emplacements géographiquement éloignés.

Techniquement les informations, y compris les données critiques sous forme non chiffrée, passent sur Internet. Une connexion VPN offre une combinaison de fonctions de chiffrement et de tunneling pour relever le défi de la sécurité. Les entreprises utilisent des protocoles de transfert de données tels qu'IPSec pour encapsuler les données transmises dans des paquets IP sur Internet.

La passerelle VPN reçoit ces données encapsulées, les déchiffre et les transmet au destinataire. Le trafic provenant de la passerelle VPN est traité comme s'il provenait d'un utilisateur sur le LAN local. Grâce à une telle connexion VPN, l'utilisateur obtient un accès complet et permanent au réseau.

2.6.3 Attentions aux vendeurs

Il faut savoir que la plupart des vendeurs de VPN ne garantissent pas un anonymat (politique de no log non respectée), pire ces derniers sont susceptibles de revendre vos données. Le mieux à faire c'est de se construire son propre VPN à partir d'un VPS et de la technologie OpenVPN, ou bien de quand même faire confiance à certains acteurs comme ProtonVPN qui est un service crée par des chercheurs du CERN.

2.7 Proxy Web

2.7.1 Pourquoi un proxy web ?

Dans le cadre plus précis des réseaux informatiques, un proxy est une solution servant d'intermédiaire pour accéder à un autre réseau, généralement Internet. Par extension, on appelle aussi « proxy » un matériel comme un serveur mis en place pour assurer le fonctionnement de tels services. Dans notre cas un proxy web va être un serveur ou une liste de serveurs qui vont nous servir de protection afin de camoufler notre adresse IP publique. Cela est utile par exemple pour faire plusieurs requêtes sur un serveur avec une adresse IP par requête.

2.7.2 Type de proxy

Les proxys SOCKS et HTTPS utilisent les protocoles correspondants (SOCKS et HTTP respectivement).

Ces types de proxys offrent presque les mêmes fonctionnalités, à la différence que le proxy SOCKS se trouve sur un port dédié et que le proxy HTTPS peut être combiné avec un proxy HTTP ou même avec un serveur HTTP (ou autre construction hybride).

Un autre avantage du proxy HTTPS est que certains administrateurs bloquent les proxys SOCKS et autorisent les connexions HTTP/HTTPS, de sorte qu'il devient possible de contourner les restrictions de NAT/firewall en utilisant un proxy HTTPS.

D'autre part, certains mandataires HTTPS sont configurés pour autoriser les connexions aux hôtes HTTP et HTTPS distants uniquement (c'est-à-dire pas aux ports personnalisés d'autres protocoles).

2.8 Navigateur

2.8.1 Navigateurs Web

Chromium : Chromium est la version libre du navigateur WEB Google Chrome. Google met en ligne une version libre de téléchargement et de distribution qui peut être utilisée par des particuliers ou entreprises pour proposer un navigateur WEB basé sur Chromium.

Chromium est compatible Windows, Mac et Linux et les extensions Google Chrome fonctionnent dessus. L'icône et le logo de Chromium reprend celui de Chrome, à part que l'icône est toute bleue.

Brave : Brave est un navigateur web open source qui a pour objectif de protéger la vie privée en bloquant par défaut les pisteurs et en favorisant une navigation via les pages en HTTPS avec l'extension HTTPS Everywhere.

Selon son créateur, il serait 40 % plus rapide que Google Chrome sur les ordinateurs et 4 fois plus rapide sur les smartphones. Cette plus grande rapidité est due aux éléments qu'il ne charge pas (pisteurs, cookies tiers et publicité en ligne).

Le navigateur est disponible sous Windows, macOS et Linux ainsi que sur iOS et Android.

Deux modes de navigation privée sont proposés :

- « **Private Window** » : mode de navigation privée « classique »
- « **Private Window via TOR** » : mode de navigation via TOR afin d'anonymiser sa connexion.

Firefox : Navigateur Open-source de la fondation Mozilla, très facile à utiliser et dispose, tout comme Chrome, d'une grande bibliothèque d'extensions et de thèmes.

2.8.2 Extensions vie privée

Voici une liste d'extensions qui va vous permettre de contrer le fingerprinting.

NoScript : NoScript est une extension qui permet de bloquer les scripts JavaScript, Java, Flash et autres plug ins des sites qui ne font pas partie de la liste blanche définie par vous. Elle permet aussi de se protéger contre les attaques XSS.

HTTPS Everywhere : L'extension HTTPS Everywhere garantit que chaque site web que vous visitez utilise le protocole HTTPS, version sécurisée du protocole HTTP habituel. Le protocole HTTPS chiffre votre connexion Internet à un site web, ce qui garantit la sécurité et la confidentialité de votre session de navigation. La connexion HTTP normale n'offre pas la même protection.

De nombreux sites sont désormais configurés pour utiliser le protocole HTTPS. Cependant, il existe encore des millions de sites web qui ne sont pas et seront par défaut en HTTP. Google Chrome affichera un avertissement lorsque vous tenterez d'accéder à un site en utilisant HTTP plutôt que HTTPS et vous demandera si vous souhaitez continuer.

Et c'est exactement là que l'extension HTTPS Everywhere est utile, pour les millions de sites qui utilisent encore le protocole HTTP.

uBlock Origin : Les annonces sont partout sur internet. Elles font tourner le Web de multiples façons, en soutenant économiquement de nombreux sites et services importants que vous utilisez chaque jour. Or, les annonces s'accompagnent d'un suivi, à travers des scripts qui enregistrent votre activité et utilisant ces données pour rationaliser les annonces que vous voyez.

Cette extension vous permet de bloquer un grand nombre de ces scripts de suivi tiers intrusifs. L'extension comprend plusieurs listes de suivi de tiers pratiques et préétablies que vous pouvez activer et désactiver. Vous pouvez aussi facilement mettre sur liste blanche d'autres sites et services (car de nombreux sites web dépendent des revenus publicitaires pour rester à flot et n'affichent pas de publicités !)

Le bonus d'uBlock Origin est son blocage de la publicité malveillante. uBlock Origin peut bloquer des domaines malveillants connus, ainsi que des domaines connus pour afficher des publicités malveillantes et autres désagréments.

Unshorten.Link : L'extension Unshorten.link fournit un service simple, mais utile. Elle permet de supprimer tout lien raccourci. Lorsqu'un lien est raccourci, il est plus facile de masquer une URL malveillante et donc de tromper quelqu'un en lui faisant cliquer sur quelque chose qu'il ne devrait pas (par exemple un IP Logger qui est un lien malveillant envoyé à une cible dans le but de récupérer son Adresse IP). Une fois installée, l'extension vous redirige vers sa page sécurisée lorsque vous cliquez sur un lien raccourci. Vous pouvez y voir l'URL cible réelle et décider si le lien est sûr ou non.

Disconnect Facebook : Facebook est bien connu pour ses problèmes de confidentialité. Comme Google, Facebook monétise vos données et les vend aux annonceurs. Mais ce n'est pas seulement sur le site de Facebook que le géant des médias sociaux aspire vos données. Tout site qui propose une option de connexion sociale vend également vos données.

2.8.3 Extensions OSINT

Voici une liste d'extensions sur Firefox pour vous faciliter vos investigations :

https://addons.mozilla.org/es/firefox/addon/wayback-machine_new/

https://addons.mozilla.org/es/firefox/addon/mitaka/?src=search

https://addons.mozilla.org/es/firefox/addon/exif-viewer/

https://addons.mozilla.org/en-US/firefox/addon/ip-address-and-domain-info/

https://addons.mozilla.org/es/firefox/addon/http-header-live/

https://addons.mozilla.org/es/firefox/addon/vulners-web-scanner/

https://addons.mozilla.org/en-US/firefox/addon/nimbus-screenshot/

2.9 Live OS

Dans cette rubrique, nous allons donc voir ce qu'est un Live OS et comment vous pouvez utiliser cette technologie pour vos investigations.

Qu'est-ce qu'un Live OS ?

Un Live OS est simplement un système d'exploitation comme les autres (exemple : Windows 10, Ubuntu, Fedora etc.…), avec pour seule différence la possibilité de pouvoir installer ce dernier sur un média amovible tel qu'une clé USB, un DVD ou un disque dur externe.

Cet OS sera non-persistant, ce qui signifie par exemple que vous pouvez avoir accès à un Ubuntu mais à la fermeture, cet OS ne sauvegardera ni les logiciels installés pendant la session, ni vos données, ni vos paramétrages particuliers.

Oui ! Vous n'avez pas besoin d'installer un Live OS sur votre poste de travail. Insérez votre média amovible sur votre PC et utilisez-le. C'est aussi simple que cela.

Vous avez terminé votre travail ? Il suffit d'éjecter votre média et aucune donnée ne sera sauvegardée sur votre PC. Cela peut être pratique dans des cas où vous ne voulez pas laisser de trace sur vos recherches ou si vous êtes dans un environnement ou installer un OS sur votre machine est impossible.

De multiples Live OS existent, en voici une liste non exhaustive :

- Kali Linux (Boite à outils pour la sécurité informatique)
- Tails (Distribution pour des sessions anonymes)
- Debian
- Ubuntu
- Fedora

2.10 Téléphonie

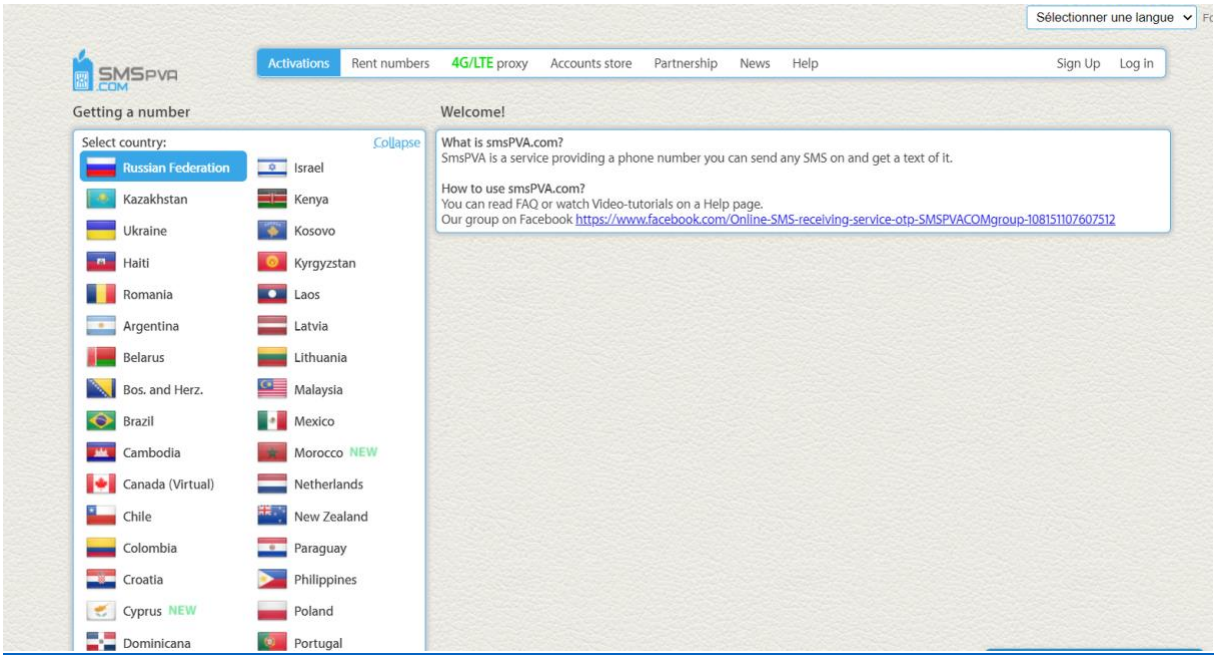
2.10.1 Double authentification

Pour pouvoir sécuriser l'accès à vos applications, comptes, etc., votre téléphone peut vous servir de moyen pour effectuer la double authentification permettant de faire face à une possible compromission de votre ordinateur ou de vos mots de passe avec des applications comme Google Authentificator.

2.10.2 Utilisation de numéros de téléphone

Plusieurs services peuvent vous aider à utiliser un autre numéro de téléphone virtuel afin de bypasser certains services sur le web demandant un numéro de téléphone pour activer ou vérifier votre compte, comme Twitter. Voici un service qui propose cela :

http://smspva.com/

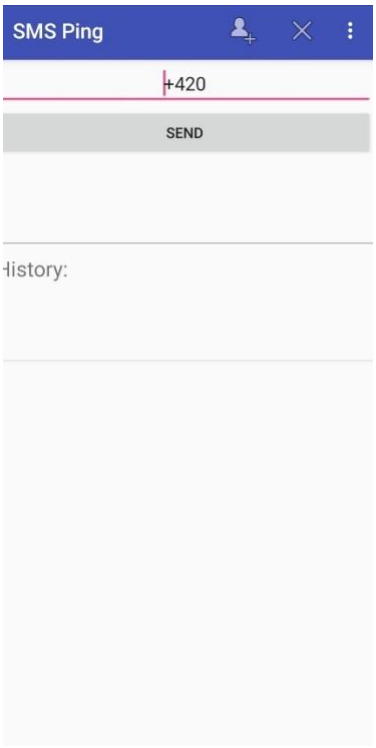


2.10.3 Vérifier si un téléphone est relié au Réseau GSM

Voici une petite technique qui permet de savoir si un téléphone est relié ou non au réseau GSM. Elle consiste a envoyé à la victime un Silent SMS.

Un Silent SMS est le plus souvent utilisé par des entités qui ont les moyens d'obtenir ce que l'on appelle des « Call Data Records », à partir d'un opérateur de téléphonie mobile. Ces données peuvent aussi être obtenues au travers du réseau dit « SS7 », qui interconnecte tous les opérateurs mobiles, et dont les accès sont difficilement maîtrisés, aux vues du nombre en perpétuelle croissance des opérateurs mobiles (et opérateurs virtuels) dans le monde.

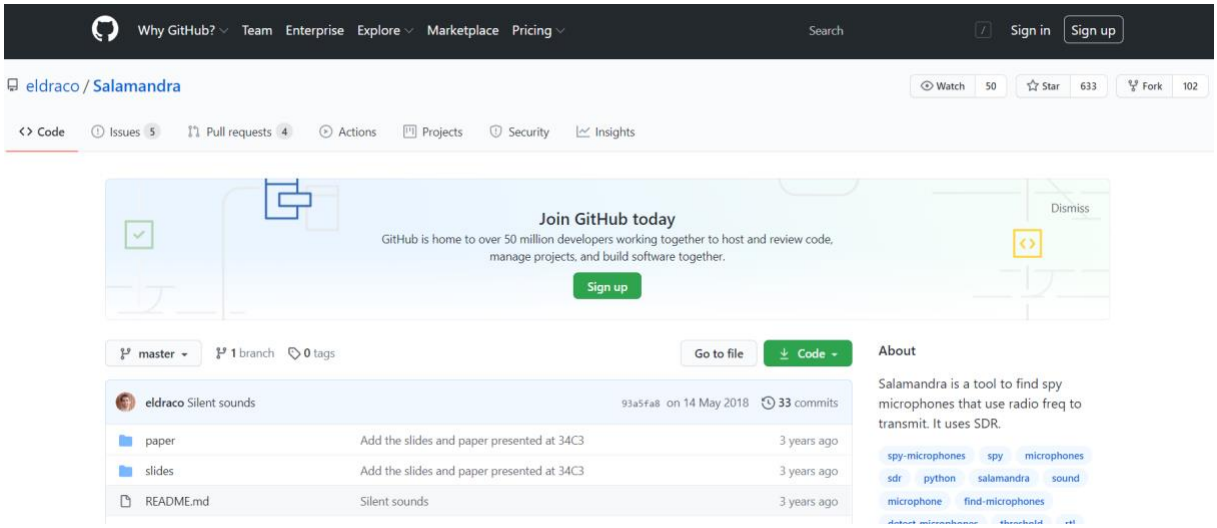
Pour cela j'utilise une application Android disponible sur F-DROID qui est un catalogue pour applications open-source, elle se nomme SMS Ping.



2.11 Vérification de micro-espion

Je vous présente Salamandra. C'est un outil permettant de détecter et de localiser les micros espions dans les environnements fermés. Il trouve les microphones en fonction de la force du signal envoyé par le microphone et de la quantité de bruit et de fréquences superposées. En se basant sur le bruit généré, il peut estimer la distance qui vous sépare du microphone.

Voici le lien du repo : https://github.com/eldraco/Salamandra

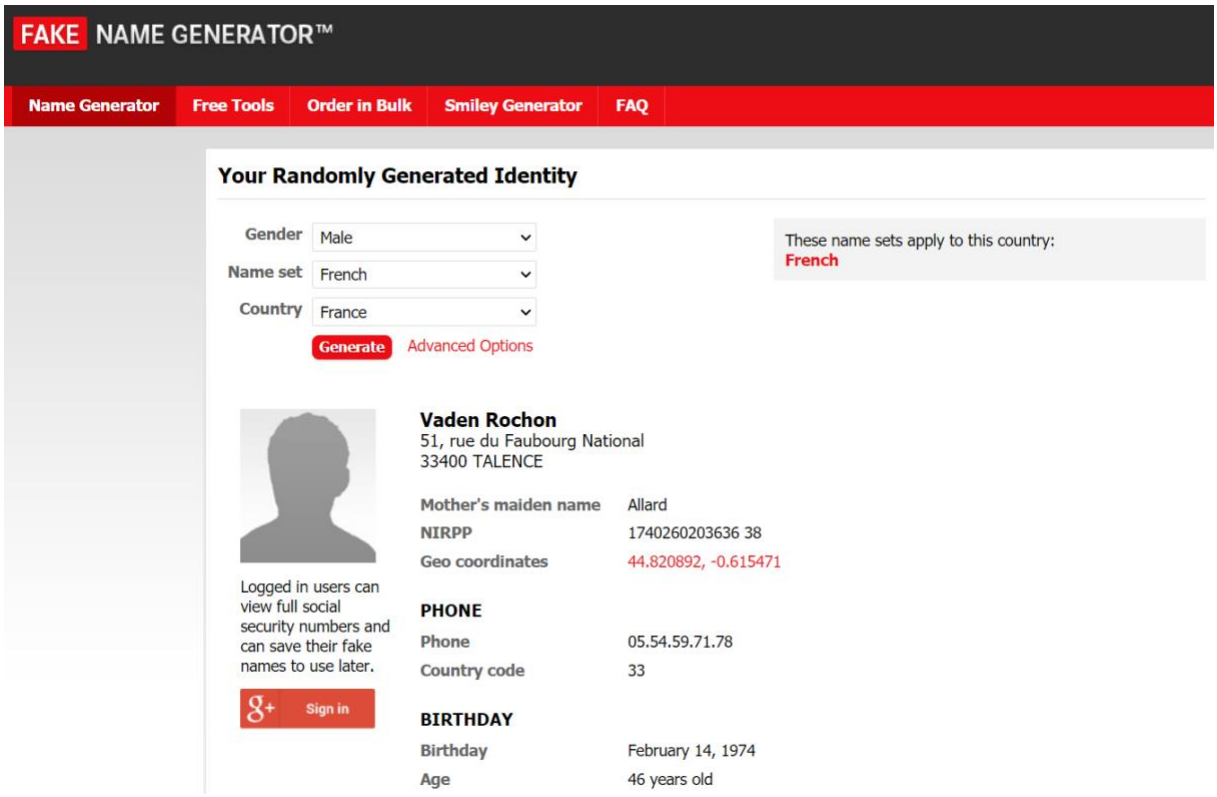


2.12 PsyOps

Pour brouiller les pistes autour de vos activités afin de contrer les potentiels attaquants voulant vous nuire, je vous recommande de créer de fausses identités avec un background réaliste grâce à des sites comme : https://www.fakenamegenerator.com/gen-random-fr-fr.php

N'hésitez pas à également laisser des pastebin avec de fausses informations personnelles afin de brouiller les pistes, ou bien mettre en évidence un semblant de croisement de données susceptible d'être trouvé par une recherche (exemple : pseudo relié à une identité réelle sur LinkedIn, faux compte twitter, Facebook, etc....)

Exemple de fausse identité créée



3 - COLLECTE ACTIVE DE RENSEIGNEMENTS

La collecte active d'informations va être détectée par la cible et les comportements suspects ou malveillants. Au cours de cette étape, votre but va être de cartographier activement l'infrastructure du réseau, recensez activement et/ou analysez les vulnérabilités des services ouverts, vous allez aussi rechercher activement les répertoires, fichiers et serveurs non publiés. La plupart de ces activités relèvent de vos activités habituelles de "reconnaissance" ou de "balayage" pour votre test d'intrusion.

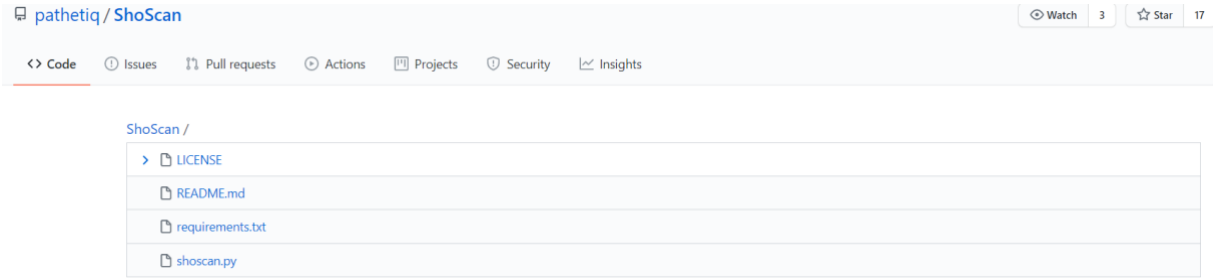
3.1 Scan de port

En informatique, le scan de ports est une technique servant à rechercher les ports ouverts sur un hôte. Cette technique est utilisée par les administrateurs des systèmes informatiques pour contrôler la sécurité des serveurs de leurs réseaux. La même technique est aussi utilisée par les pirates informatiques pour tenter de trouver des failles dans des systèmes informatiques.

Les scans de ports se font habituellement sur le protocole TCP ; néanmoins, certains logiciels permettent aussi d'effectuer des balayages UDP & ICMP. Cette dernière fonctionnalité est beaucoup moins fiable, UDP étant orienté sans connexion, le service ne répondra que si la requête correspond à un modèle précis variant selon le logiciel serveur utilisé.

Je vous donne ci-dessous deux techniques permettant de faire du scan de ports :

- **Via Shodan** : c'est un script qui va vous permettre de faire un scan de ports sur de multiples adresses IP en utilisant l'API de Shodan pour effectuer cette manœuvre : https://github.com/pathetiq/ShoScan



- **Via NMAP** : Nmap utilise les paquets (ICMP, UDP, TCP SYN…) pour déterminer quels hôtes sont disponibles sur le réseau, quels services (nom et version de l'application) ces hôtes offrent, quels systèmes d'exploitation, la version qu'ils utilisent, quel type de filtres de paquets/pare-feux sont utilisés, et des dizaines d'autres caractéristiques. En plus de l'exécutable classique Nmap en ligne de commande, la suite Nmap comprend une interface graphique avancée et un visualiseur de résultats (Zenmap), un outil flexible de transfert, de redirection et de débogage des données (Ncat), un utilitaire de comparaison des résultats d'analyse (Ndiff) et un outil de génération de paquets et d'analyse des réponses (Nping) : https://nmap.org/

3.2 DNS

L'énumération DNS est l'une des tâches de reconnaissance les plus populaires pour établir le profil de votre cible. Il s'agit de détecter et d'énumérer tous les enregistrements DNS possibles d'un nom de domaine. Cela inclut les noms d'hôtes, les noms d'enregistrements DNS, les types d'enregistrements DNS, les TTL, les adresses IP et un peu plus, selon la quantité d'informations que vous recherchez.

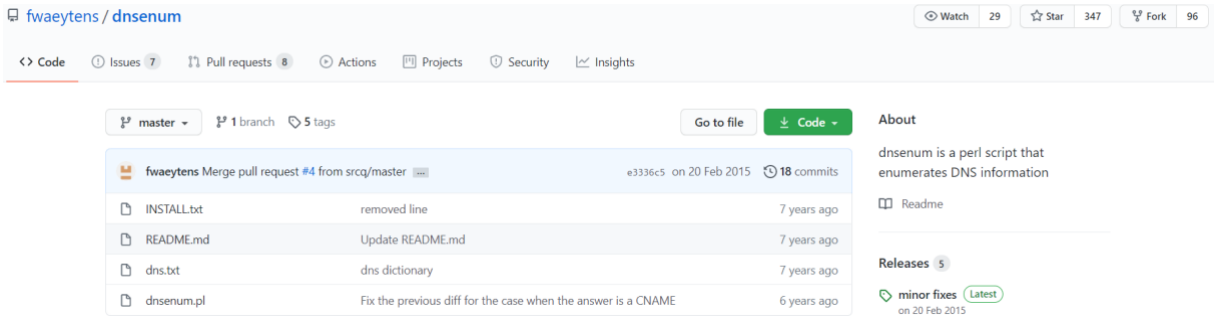
Grâce à une énumération efficace des DNS, vous pouvez cloner les zones DNS manuellement, à l'aide de scripts ou en exploitant les vulnérabilités de transfert de zone DNS, connu sous le nom de transfert AXFR (Asynchronous Transfer Full Range). Ce dernier type de transfert DNS a lieu lorsqu'un attaquant détecte un serveur DNS mal configuré qui répond en fait à des requêtes AXFR.

Vous pouvez vérifier si des enregistrements SPF et DMARC sont présents pour détecter les configurations faibles qui permettent d'usurper un domaine par exemple.

Voici une liste de tools pour vous aider dans l'énumération DNS :

- **Dig** : Est un résolveur DNS UNIX, voici un exemple sur l'exploitation d'un transfert de zone :

- **Host & nslookup** : Host et Nslookup sont des commandes utilisées pour résoudre l'adresse IP de tout nom de domaine donné au préalable et vice versa.
- **DNSenum** : DNSEnum est un script écrit en Perl qui peut vous aider à créer une carte DNS complète de n'importe quel nom de domaine sur l'Internet : https://github.com/fwaeytens/dnsenum



- **Nmap avec le script dns-brute** : Voici un exemple sur le domaine **google.com** :

```
root@debian:~# nmap -T4 -p 53 --script dns-brute google.com
Starting Nmap 7.70 ( https://nmap.org ) at 2020-10-15 10:44 EDT
Nmap scan report for google.com (216.58.214.78)
Host is up (0.10s latency).
Other addresses for google.com (not scanned): 2a00:1450:4007:80b::200e
rDNS record for 216.58.214.78: [redacted]

PORT   STATE    SERVICE
53/tcp filtered domain

Host script results:
| dns-brute:
|   DNS Brute-force hostnames:
|     admin.google.com - 216.58.215.46
|     admin.google.com - 2a00:1450:4007:808:0:0:0:200e
|     id.google.com - 216.58.201.163
|     ads.google.com - 172.217.19.238
|     id.google.com - 2404:6800:4003:c04:0:0:0:5e
|     ads.google.com - 2a00:1450:4007:806:0:0:0:200e
|     images.google.com - 216.58.213.78
|     images.google.com - 2a00:1450:4007:810:0:0:0:200e
|     news.google.com - 216.58.198.206
|     alerts.google.com - 172.217.18.206
|     news.google.com - 2a00:1450:4007:812:0:0:0:200e
|     alerts.google.com - 2a00:1450:4007:805:0:0:0:200e
```

- DNSRecon : https://github.com/darkoperator/dnsrecon
- Fierce : https://github.com/mschwager/fierce
- Spoofcheck : Il s'agit d'un programme qui vérifie si un domaine peut être usurpé. Le programme vérifie les enregistrements SPF et DMARC pour les configurations faibles qui permettent l'usurpation : https://github.com/BishopFox/spoofcheck

3.3 Domaine

Sublist3r : Exemple de recherche sur le domaine facebook.com.

```
osint@kali:~$ sublist3r -d facebook.com
   OSINT-Sea...

                 # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for facebook.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
```

3.4 Autres axes de collecte

HTTP Header :

Les en-têtes HTTP font référence aux informations essentielles servies par le serveur web qui héberge la page web que vous essayez de parcourir.

Scan de vulnérabilités :

Sn1per : un scanner automatique de reconnaissance pour le pentest : https://github.com/1N3/Sn1per

Metasploit : Metasploit est un projet en relation avec la sécurité des systèmes informatiques. Son but est de fournir des informations sur les vulnérabilités de systèmes informatiques, d'aider à la pénétration et au développement de signatures pour les systèmes de détection d'intrusion : https://www.metasploit.com/

Dirsearch : un simple outil en ligne de commande conçu pour forcer les répertoires et les fichiers des sites web. https://github.com/maurosoria/dirsearch

Nessus : Scanner de vulnérabilités : https://fr.tenable.com/products/nessus

4 - COLLECTE PASSIVE DE RENSEIGNEMENTS

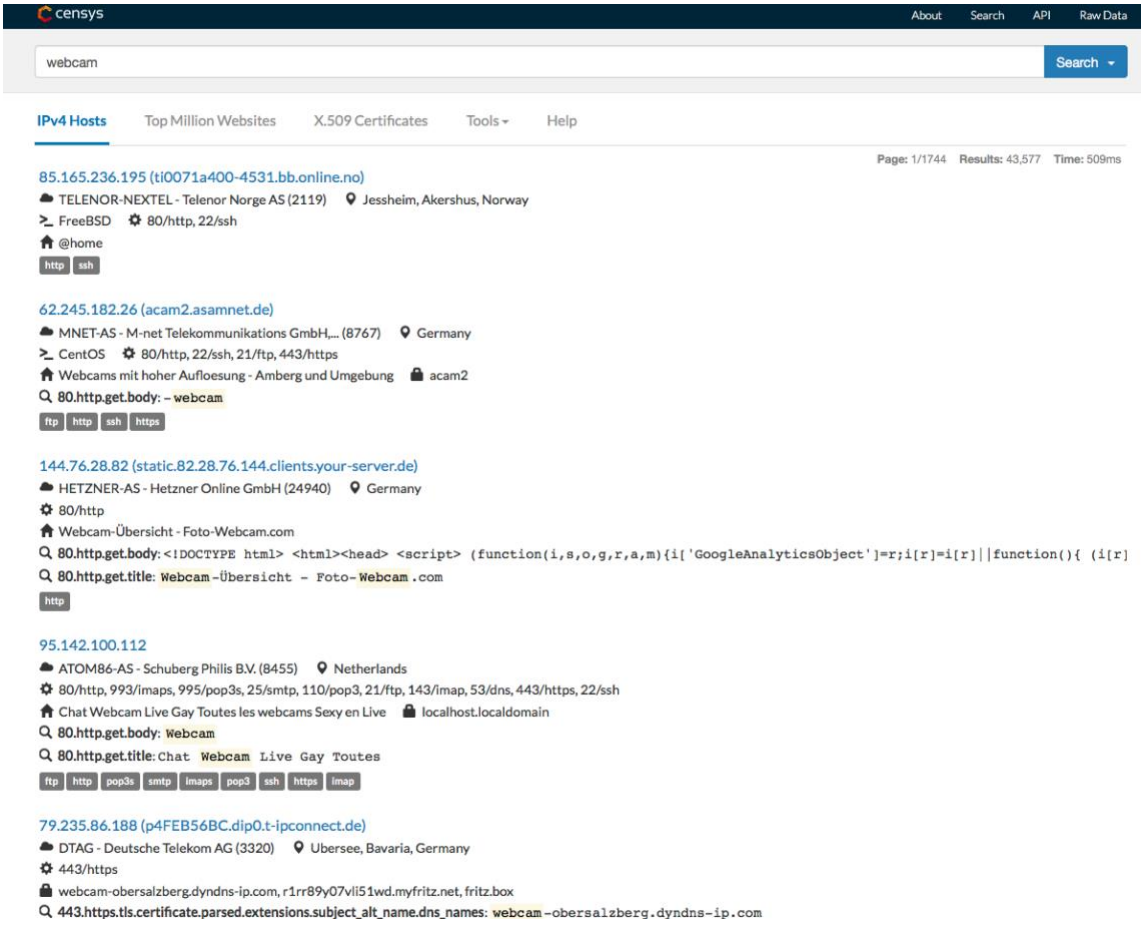
La collecte passive d'informations n'est généralement utile que s'il existe une exigence très claire selon laquelle les activités de collecte d'informations ne doivent jamais être détectées par la cible.

Ce type de profilage est techniquement difficile à réaliser, car nous n'envoyons jamais de trafic vers la cible ni à partir d'un de nos hôtes ou d'hôtes ou services "anonymes" sur l'internet. Cela signifie que nous ne pouvons qu'utiliser et recueillir des informations archivées ou stockées. Ces informations peuvent donc être obsolètes ou incorrectes, car nous sommes limités aux résultats obtenus auprès d'un tiers.

Voici une liste de tools pour vous permettre de passer par des tiers afin de recueillir des informations sur les axes divers et variés :

- pwnedOrNot est un script python qui vérifie si le compte de courrier électronique a été compromis lors d'une violation de données. Si le compte de courrier électronique est compromis, il procède à la recherche des mots de passe du compte compromis. https://github.com/thewhiteh4t/pwnedOrNot
- pwndb est un outil en ligne de commande python permettant de rechercher des informations d'identification divulguées en utilisant le service Onion du même nom. https://github.com/davidtavarez/pwndb/
- Social_Mapper est un tool qui va prendre une liste de noms et d'images (exemple LinkedIn) et va effectuer une recherche automatique de cibles à grande échelle sur de multiples sites de médias sociaux. Il produit des rapports pour aider à corréler les cibles entre les sites : https://github.com/SpiderLabs/social_mapper
- skiptracer, est un tool de type scraping web écrit en python (avec le module BeautifulSoup), il permet d'avoir des informations à caractères personnelles via des sites payants afin de compiler des informations passives sur une cible. https://github.com/xillwillx/skiptracer
- theHarvester est un outil permettant de rassembler des noms de sous-domaines, des adresses électroniques, des hôtes virtuels, des ports/bannières ouverts et des noms d'employés provenant de différentes sources publiques : https://github.com/laramies/theHarvester
- FOCA (Fingerprinting Organizations with Collected Archives) est un outil utilisé principalement pour trouver des métadonnées et des informations cachées dans les documents qu'il scanne. https://github.com/ElevenPaths/FOCA
- truffleHog recherche des infos dans les dépôts de github, en creusant profondément dans l'historique et les branches des commit. https://github.com/dxa4481/truffleHog
- GitHarvester Cet outil est utilisé pour récolter des informations de GitHub comme google dork. https://github.com/metac0rtex/GitHarvester
- Just-Metadata est un outil qui recueille et analyse les métadonnées relatives aux adresses IP. Il tente de trouver des relations entre les systèmes au sein d'un vaste ensemble de données. https://github.com/ChrisTruncer/Just-Metadata
- SimplyEmail, tool pour les mails rapide et facile à utiliser, avec un cadre sur lequel s'appuyer. https://github.com/killswitch-GUI/SimplyEmail
- Metagoofil est un outil permettant d'extraire les métadonnées des documents publics (pdf,doc,xls,ppt,etc) disponibles sur les sites web cibles. https://github.com/laramies/metagoofil
- typofinder : un outil de recherche de domaines indiquant le pays de l'adresse IP. https://github.com/nccgroup/typofinder

- findomain est un outil de recensement rapide des domaines qui utilise les journaux Certificate Transparency et une sélection d'API : https://github.com/Edu4rdSHL/findomain
- Censys est un moteur de recherche lancé par des chercheurs de l'Université du Michigan, qui collecte toutes les données qu'il peut sur les appareils connectés en IPv4 sur le net. Pour cela, il utilise le scanner de ports open source ZMap et stocke tout ce qu'il récupère dans une base de données, qui est ensuite accessible via une interface web, une API ou carrément des listings en texte brut à télécharger. Vous pouvez faire une recherche par mots clés, par IP, nom de domaines, protocole utilisé, par certificat…etc. Les informations collectées sont d'ailleurs très complètes et peuvent servir à débusquer d'éventuels problèmes de sécurité : https://censys.io/



5 - FRAMEWORKS

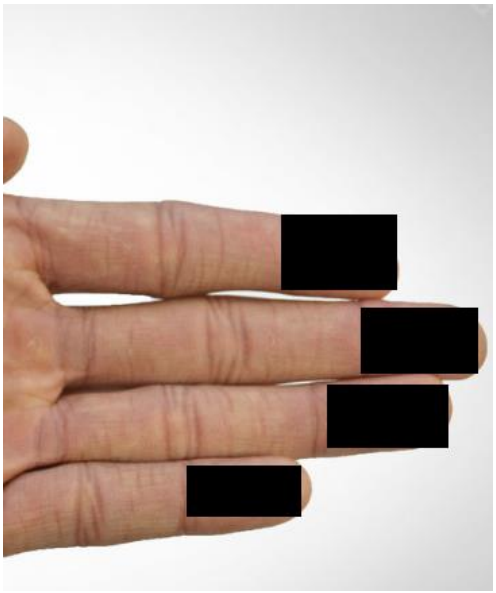
Je vais vous donner dans cette rubrique ici une liste de Framework comportant énormément d'utilités et de méthodes de recherche ainsi que de visualisations pour vos investigations :

- **Maltego** est une plateforme unique développée pour donner une image claire des menaces qui pèsent sur l'environnement que possède et exploite une organisation. Elle est sympa pour bosser en équipe : https://www.paterva.com/web7/downloads.php
- **SpiderFoot**, est un outil open source de collecte de renseignements et d'empreintes. https://github.com/smicallef/spiderfoot
- **Recon-ng** est un Framework complet de reconnaissance du Web écrit en Python. https://bitbucket.org/LaNMaSteR53/recon-ng
- **Dataspoit** est un Framework permettant d'effectuer diverses techniques de reconnaissance sur les entreprises, des particuliers, des numéros de téléphone, des adresses Bitcoin, etc., d'agréger toutes les données brutes et de fournir des données dans plusieurs formats : https://github.com/DataSploit/dataspoit

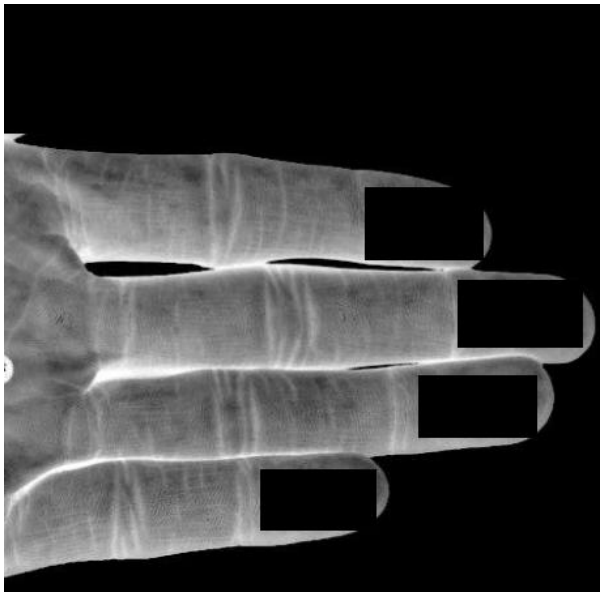
6 - EMPREINTES DIGITALES

Il est possible à partir d'une photo de vos mains de récupérer avec différentes manipulations, vos empreintes digitales.

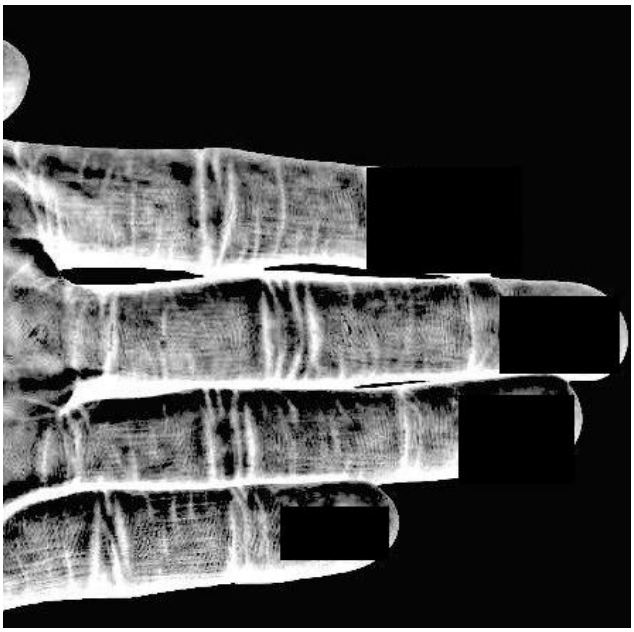
Voici un mode d'emploi sur une méthode que j'ai pu voir lors d'une conférence :



Avec le logiciel open-source GIMP, vous allez pouvoir récupérer la trace des empreintes digitales, tout d'abord vous allez désaturer l'image puis inverser les couleurs.



Ensuite vous allez améliorer la netteté de l'image, puis balancer avec le taux de contraste ainsi que le niveau d'exposition afin d'apercevoir les lignes le plus nettement possible.



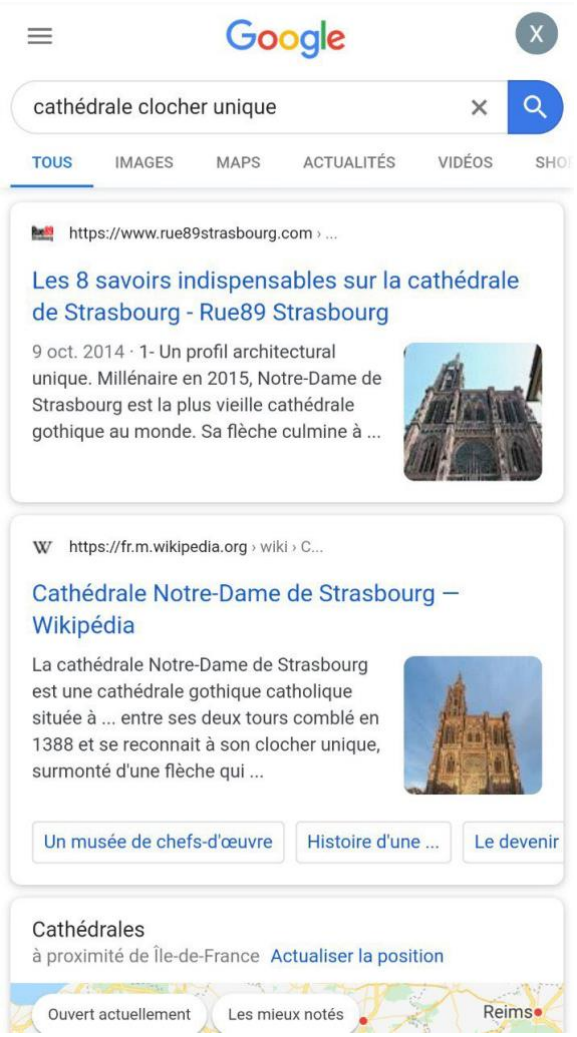
7 - INVESTIGATIONS SUR MEDIAS

7.1 GEOINT

Le terme GEOINT (Géospatial Intelligence) définit l'art de localiser précisément l'endroit ou une image ou tout autre média a pu être pris. Je vais vous montrer quelques cas sur comment j'ai pu localiser des médias de façon précise :

7.1.1 Cas 1

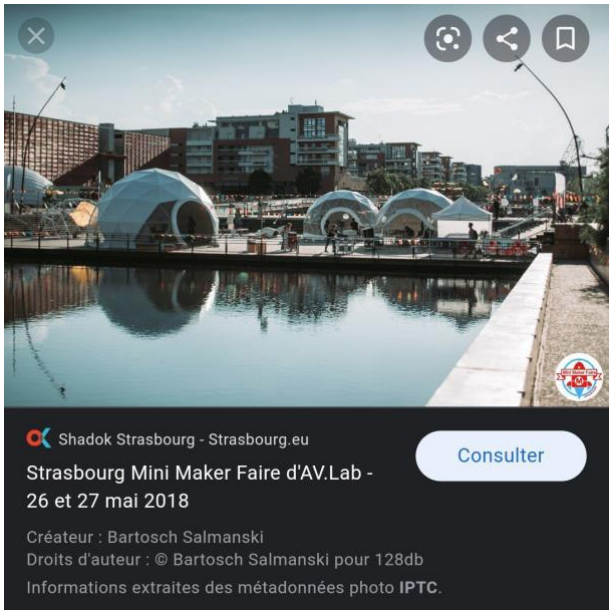
Je me concentre tout d'abord sur la cathédrale :



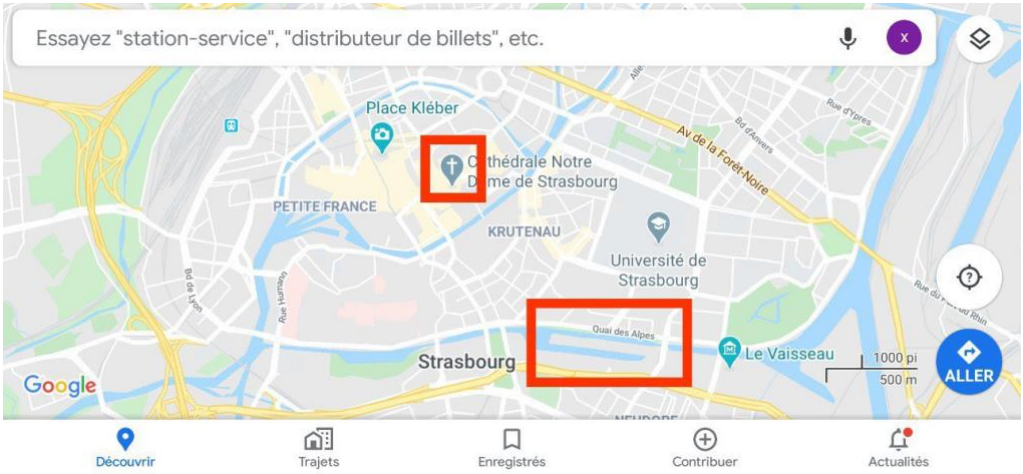
Je remarque que la ville est Strasbourg, maintenant j'effectue un repérage des canaux et des bassins

Je remarque une étrange structure à gauche :

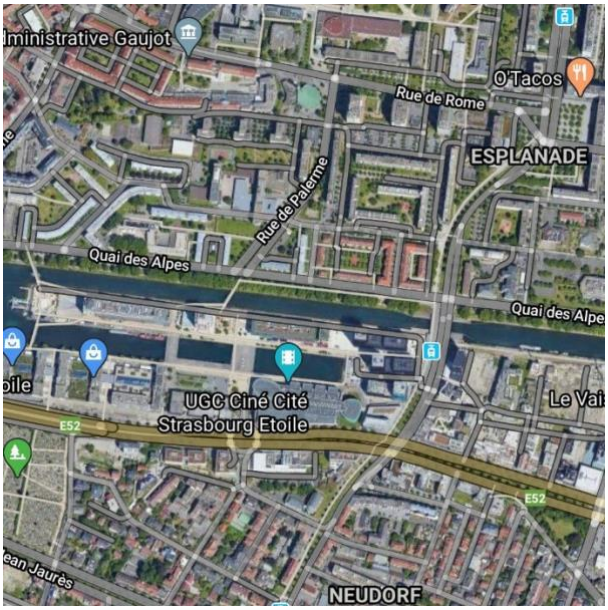
Une recherche google me donne la date de prise de vue.

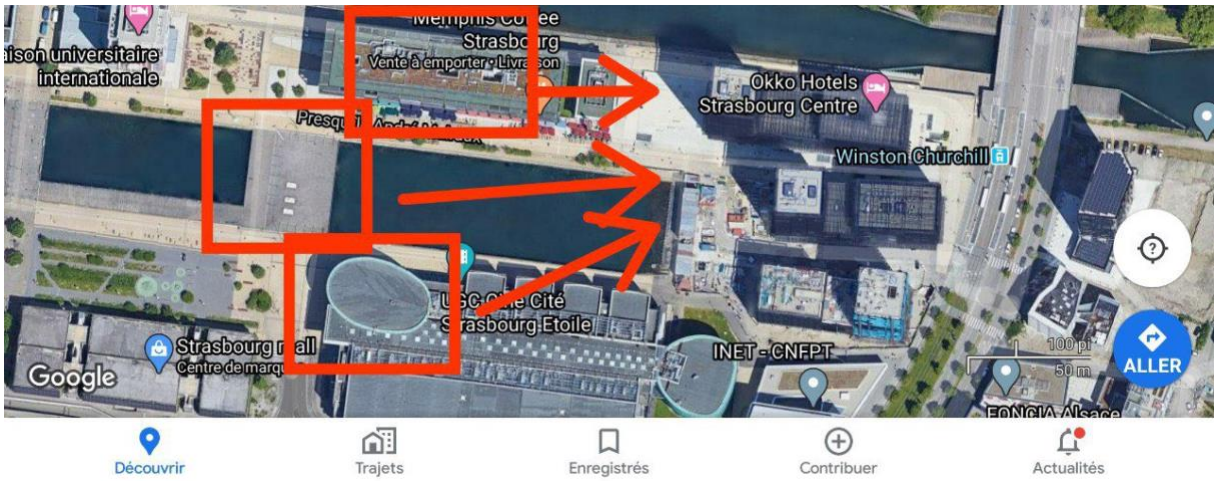


J'effectue par la suite un repérage sur Maps pour situer l'endroit exact de la prise de vue :



Je passe en mode satellite :





Maintenant je passe en mode Street-View :

On peut voir que la photo a été prise exactement à cet endroit :

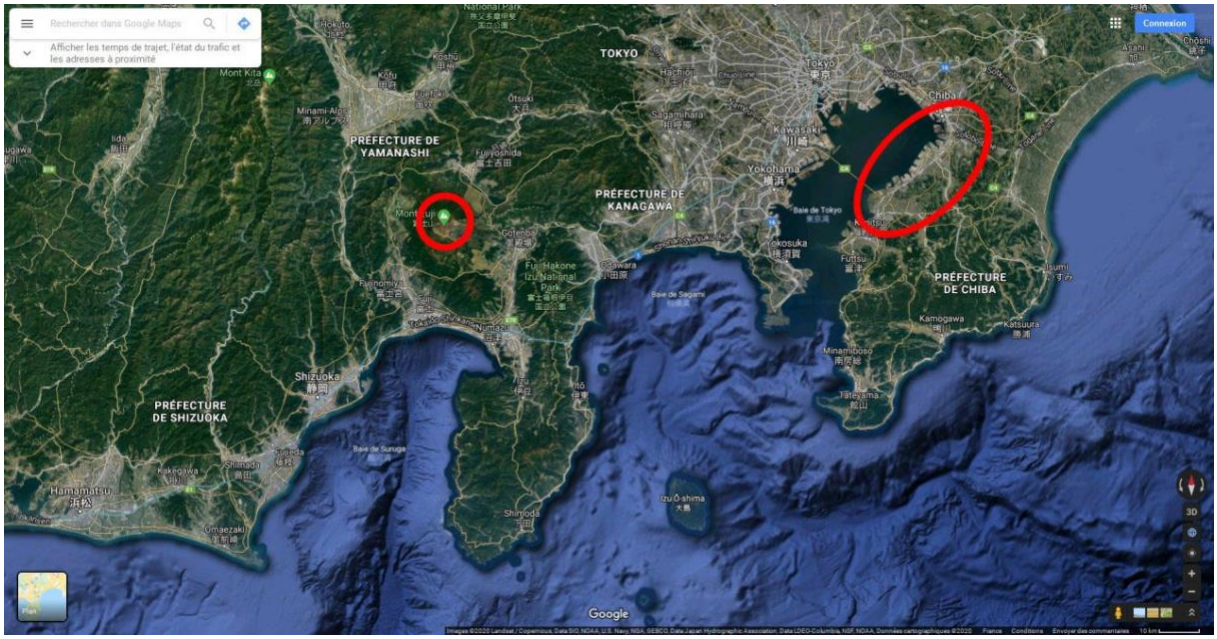
7.1.2 Cas 2

Première photo :

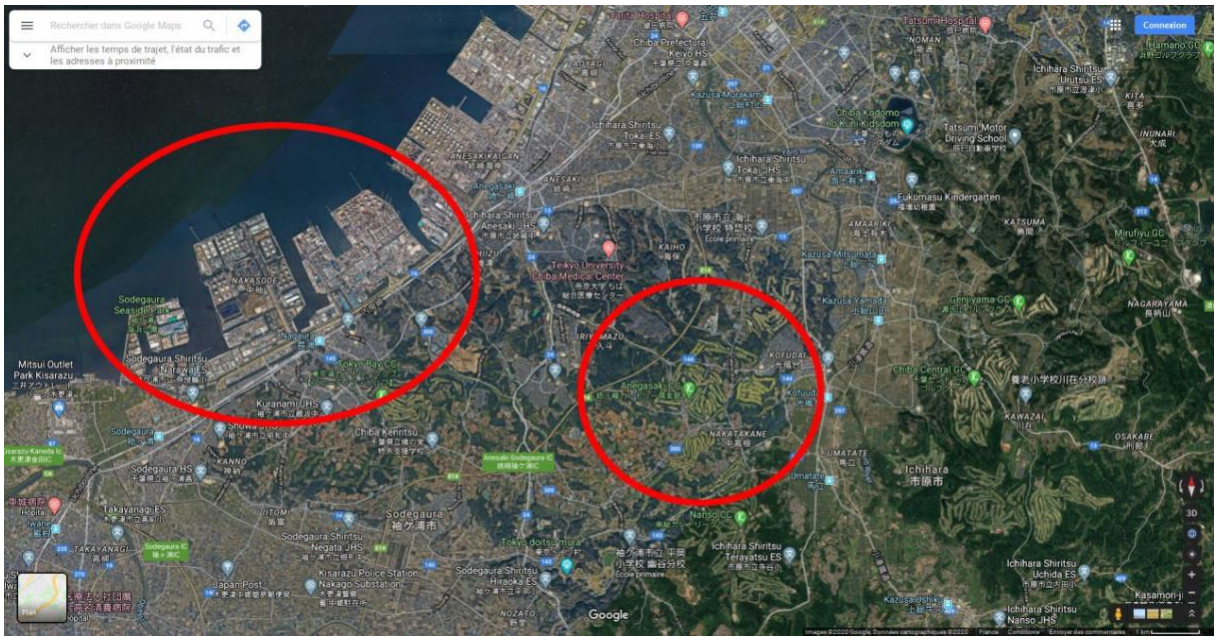
Tout d'abord je remarque 3 détails importants :

- Montagne au fond (Mont Fuji ?).
- Port d'hydrocarbures avec bassins en L.
- Grande zone grise le long de la route et parcelles de terrain enchevêtrées.

Je passe maintenant sur Maps pour avoir une vue sur le Mont Fuji, la zone de docks pouvant ressembler au port ainsi que le bras de mer orienté dans le bon sens.



J’effectue un zoom sur zone, je repère les bassins du port en L ainsi que les parcelles enchevêtrées à proximité de la route.



Maintenant je passe en 3D en m'orientant vers le Mont Fuji, voilà la position ou la photo a été prise, l’avion était dirigé vers le sud-sud-est.

Deuxième photo :

Comme Tokyo est à l'arrivée, et non pas au décollage, l'avion venait globalement par le nord. Donc je sais que le départ s'est fait dans l'hémisphère nord. Mon hypothèse : défi lancé par un gars de Strasbourg, donc voyage Strasbourg – Tokyo, je recherche les meilleures options pour aller à Tokyo depuis Strasbourg. Je trouve que le meilleur compromis pour la durée + navette = décollage Francfort. Je recherche des vols Francfort – Tokyo. Je note que l'arrivée à Tokyo s'est faite de jour (photo #2 prises au coucher du soleil : vol de nuit, arrivée à Tokyo en début de journée.)

Une seule option : vol Nippon Airlines NH204 avion B787 (l'extrémité de l'aile semble correspondre) décollage Francfort autour de 14H00 atterrissage Tokyo autour de 8H30 (semble correspondre à la photo #1).

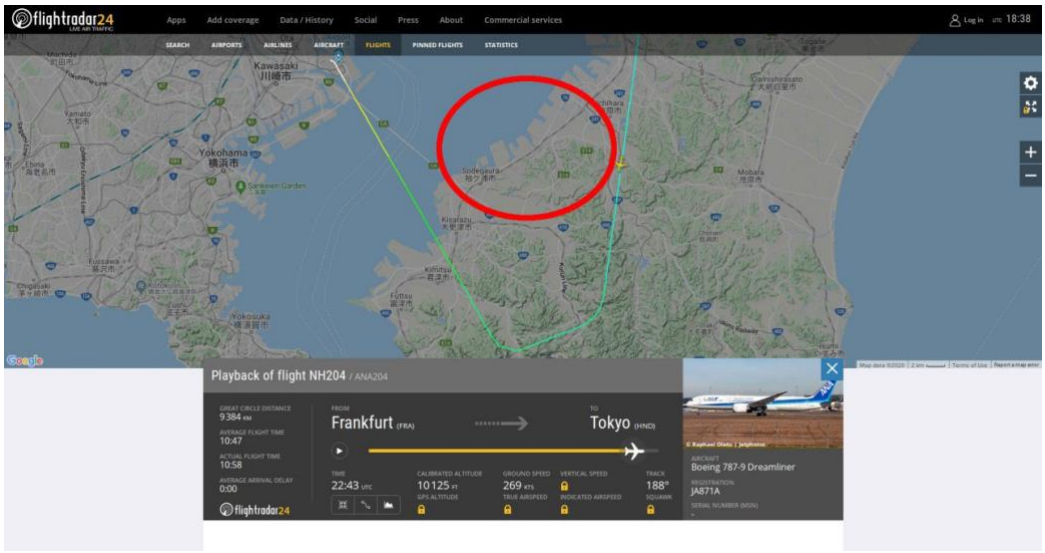
Maintenant, je note pour la photo 2 que :

- Prise au coucher de soleil dans l'hémisphère nord,
- Aux environs de la moitié du trajet (tombée de la nuit),
- Paysage très sec et enneigé,
- Rivière tortueuse sur fond de vallée plate,
- Sommets des montagnes "rabotés",
- Donc zone d'érosion par de gigantesques glaciers.

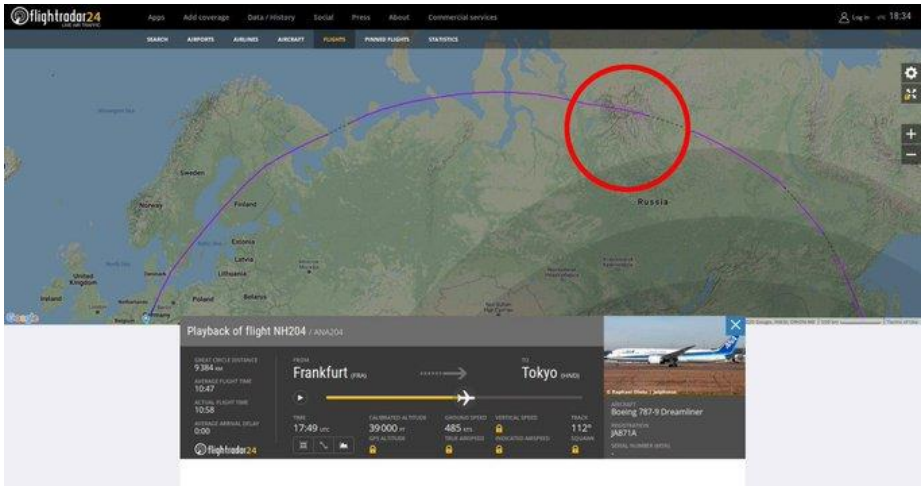
J'émet une hypothèse sur la zone : La Sibérie

J'affine mon hypothèse par FlightRadar24 (outil pour voir en temps réel des vols) pour le vol NH204. Je compare sur plusieurs vols : les routes peuvent varier selon la météo. Je recherche ensuite des zones montagneuses sèches et érodées sur la route.

D'abord je vérifie que la trajectoire finale du vol correspond sur Tokyo :

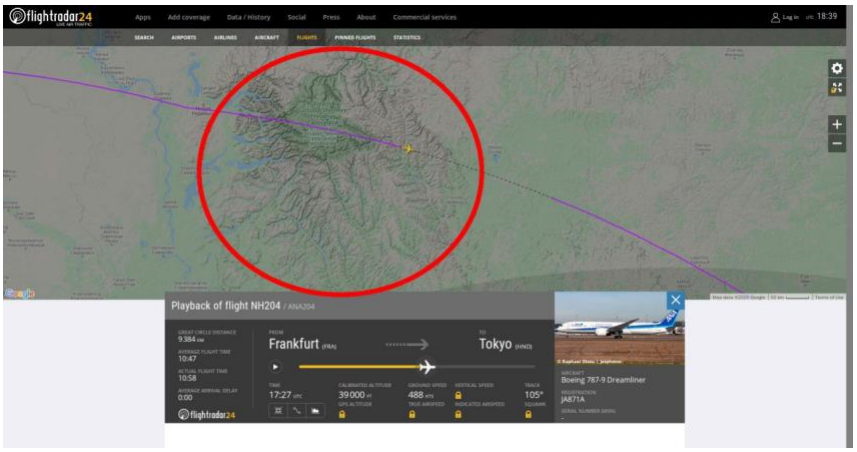


Ensuite j'analyse de la route survolant des zones montagneuses en Sibérie :

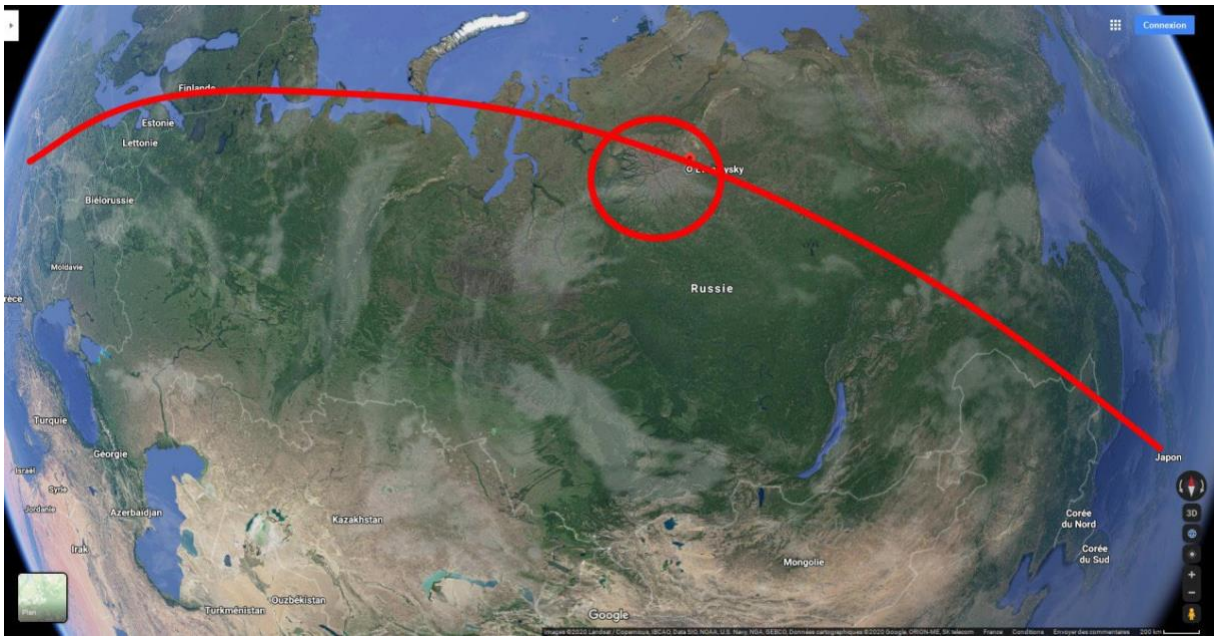


Notez la zone grise correspond au début de la nuit (variable selon les périodes de l'année, mais globalement dans le bon secteur).

On affine encore sur FR24 : (Zone d'environ 200km x 300km) :



Je passe sur Maps en mode 3D satellite :

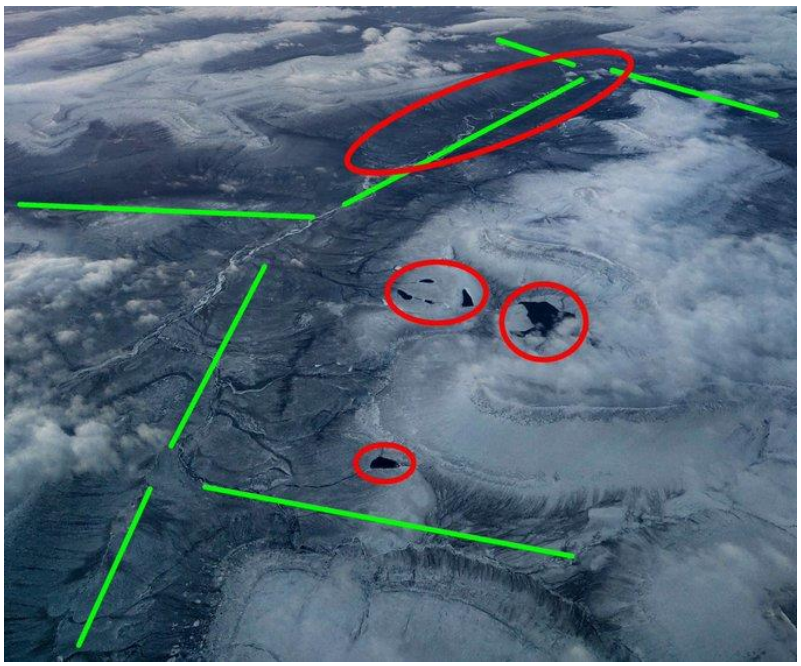


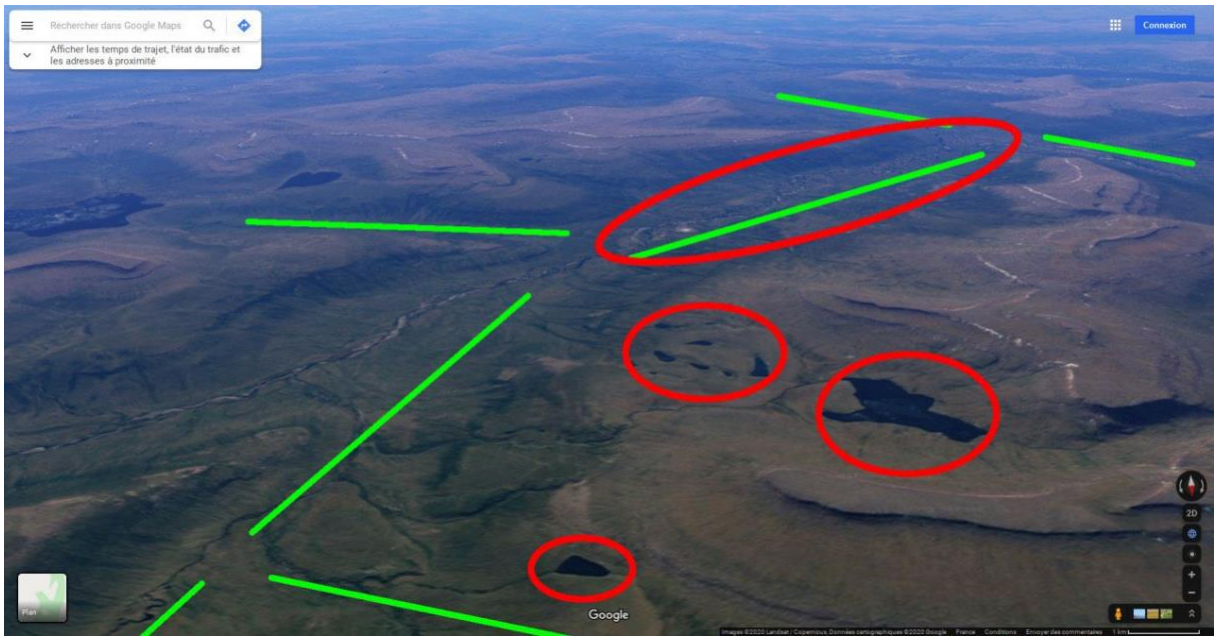
Rappels :

- Avion dirigé vers sud-est-est
- Vue dirigée vers sud-ouest (cf. position par rapport à l'aile)

A présent je navigue sur la zone en mode 3D à altitude moyenne en étant orienté vers le sud-ouest (axe de la photo).

- Rouge = détails à retrouver sur GMaps
- Vert = orientation des vallées et jonctions





Position :
https://google.de/maps/@68.4552973,99.072536,5055a,35y,183.87h,69t/data=!3m1!1e3!5m1!1e4

- Vue : orientée vers le sud-ouest (direction du coucher de soleil, avion très au nord)
- Avion : dirigé vers le sud-est-est

7.2 Reverse Image

La recherche d'images inversée est l'une des techniques d'investigation numérique les plus connues et les plus faciles. Cette méthode a également été largement utilisée dans la culture populaire grâce aux nombreux journalistes qui debunk des fakes news.

Cependant, si vous n'utilisez Google que pour la recherche d'images inversées, vous serez le plus souvent déçu. Limiter votre processus de recherche au téléchargement d'une photographie dans sa forme originale sur le seul site https://images.google.com/ peut vous donner des résultats utiles pour les images les plus manifestement volées ou les plus populaires, mais pour la plupart des projets de recherche sophistiqués, vous avez besoin de sites supplémentaires à votre disposition - ainsi que de beaucoup de créativité.

Yandex est de loin le meilleur moteur de recherche d'images inversées, avec une capacité effrayante et puissante à reconnaître les visages, les paysages et les objets, pour des résultats remarquablement précis avec des requêtes de reconnaissance des visages et des paysages.

Ses points forts résident dans les photographies prises dans un contexte européen ou ex-soviétique. Bien que les photographies d'Amérique du Nord, d'Afrique et d'autres endroits puissent encore donner des résultats utiles sur Yandex, vous pouvez vous sentir frustré en faisant défiler les résultats principalement de Russie, d'Ukraine et d'Europe de l'Est plutôt que du pays de vos images cibles.

Les algorithmes de reconnaissance faciale utilisés par Yandex sont étonnamment bons. Non seulement Yandex recherchera des photos qui ressemblent à celle qui contient un visage, mais il cherchera également d'autres photos de la même personne (déterminées par la correspondance des similitudes faciales) avec un éclairage, des couleurs de fond et des positions complètement différents. Alors que Google et Bing peuvent se contenter de rechercher d'autres photographies montrant une personne avec des vêtements et des traits faciaux généraux similaires, Yandex recherchera ces correspondances, ainsi que d'autres photographies d'une correspondance faciale. Attention, depuis quelque temps, les résultats de Yandex ne sont pas aussi pertinents qu'auparavant. Plusieurs membres de la communauté OSINT trouvent que Yandex fonctionne mieux lorsque l'on a un VPN connecté sur un serveur Russe.

Bing et Google sont aussi très bons, mais pas aussi avancés que Yandex.

Google Lens par contre est excellent pour reverse des paysages, car il embarque de l'IA avec un algorithme de reconnaissance.

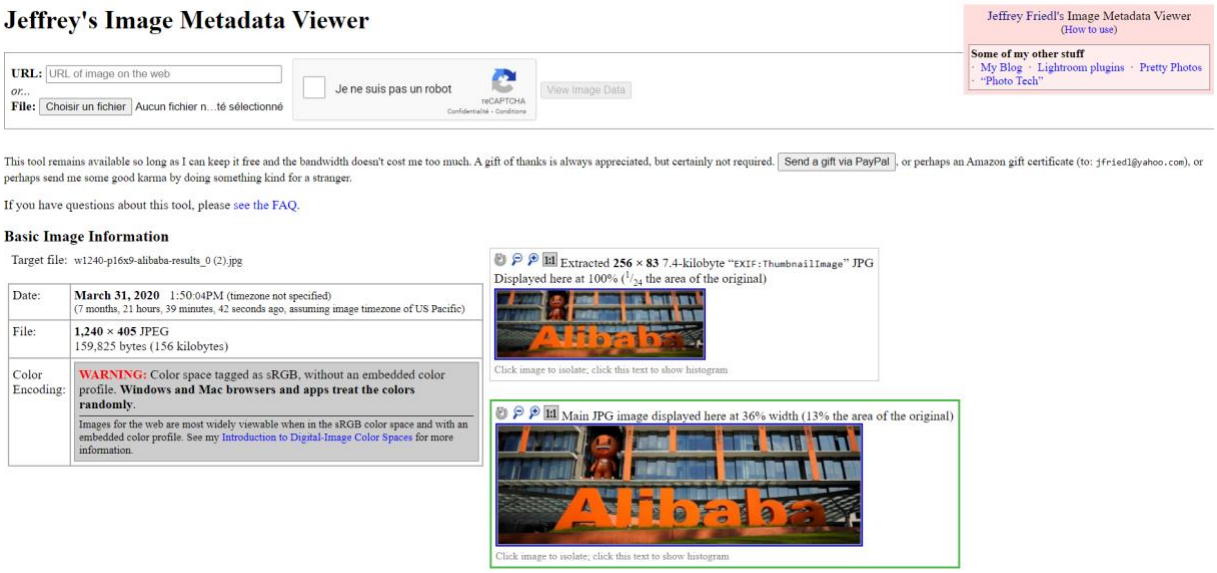
7.3 Métadonnées

Les métadonnées EXIF sont des informations contenues dans des fichiers image (jpeg généralement), qui permettent de fournir des informations techniques sur un cliché, notamment les paramètres de l'appareil photographique :

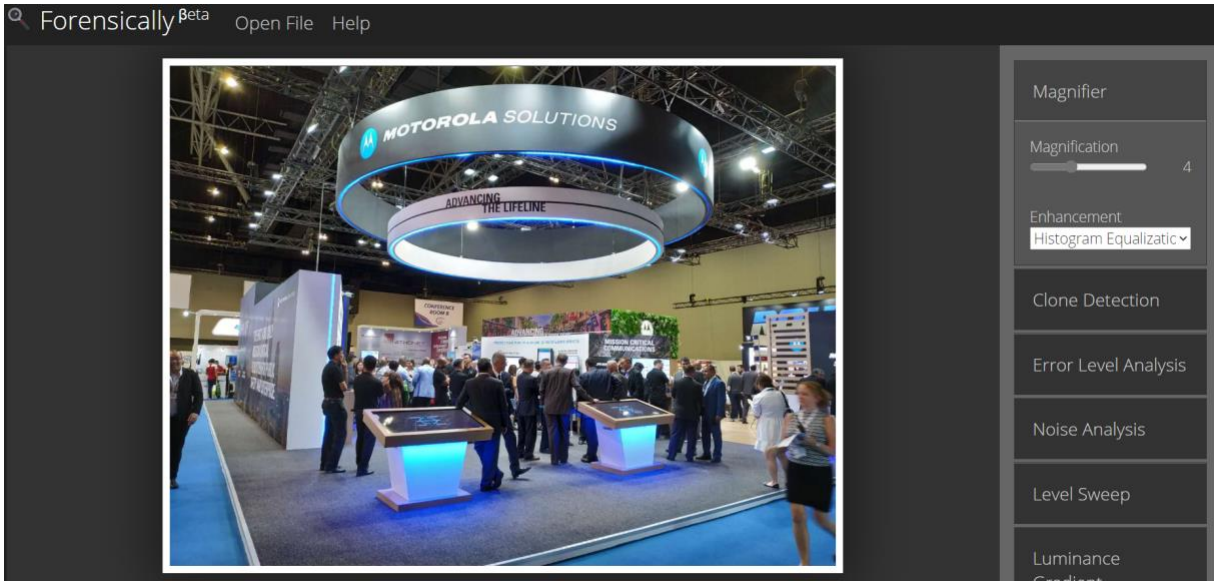
- Marque et Modèle
- Date du cliché
- Vitesse d'obturation
- Exposition
- Ouverture du diaphragme
- Sensibilité (ISO)
- Distance focale
- Objectif
- Flash activé ou désactivé
- Source lumineuse
- Coordonnées

Voici un site pour extraire les données EXIF d'une image : http://exif.regex.info/exif.cgi

Exemple d'une recherche sur la plateforme



Je vous donne aussi un lien d'un site afin d'analyser une image avec différents tests permettant de savoir si des éléments sur l'image ont été modifiés, le site propose aussi une extraction des métadonnées : https://29a.ch/photo-forensics/#forensic-magnifier



8 - SOCIAL ENGINEERING

L'ingénierie sociale (social engineering en anglais) est, dans le contexte de la sécurité de l'information, une pratique de manipulation psychologique à des fins d'escroquerie. Les termes plus appropriés à utiliser sont le piratage psychologique ou la fraude psychologique. Dans le contexte de la sécurité de l'information, la désignation ingénierie sociale est déconseillée puisqu'elle n'accentue pas le concept de tromperie.

8.1 Campagne de phishing

Simuler des campagnes de phishing permet de déterminer le risque d'exposition réel au niveau de votre organisme, et ainsi, sensibiliser de manière efficace vos collaborateurs

Cela va vous permettre aussi de :

- Vous sensibiliser aux mails frauduleux.
- Adopter les bonnes pratiques face au phishing.

Nous allons utiliser l'outil Gophish, c'est un outil de phishing open-source conçu pour les entreprises et les auditeurs. Il permet de mettre en place et d'exécuter rapidement et facilement des campagnes de phishing et des formations de sensibilisation à la sécurité.

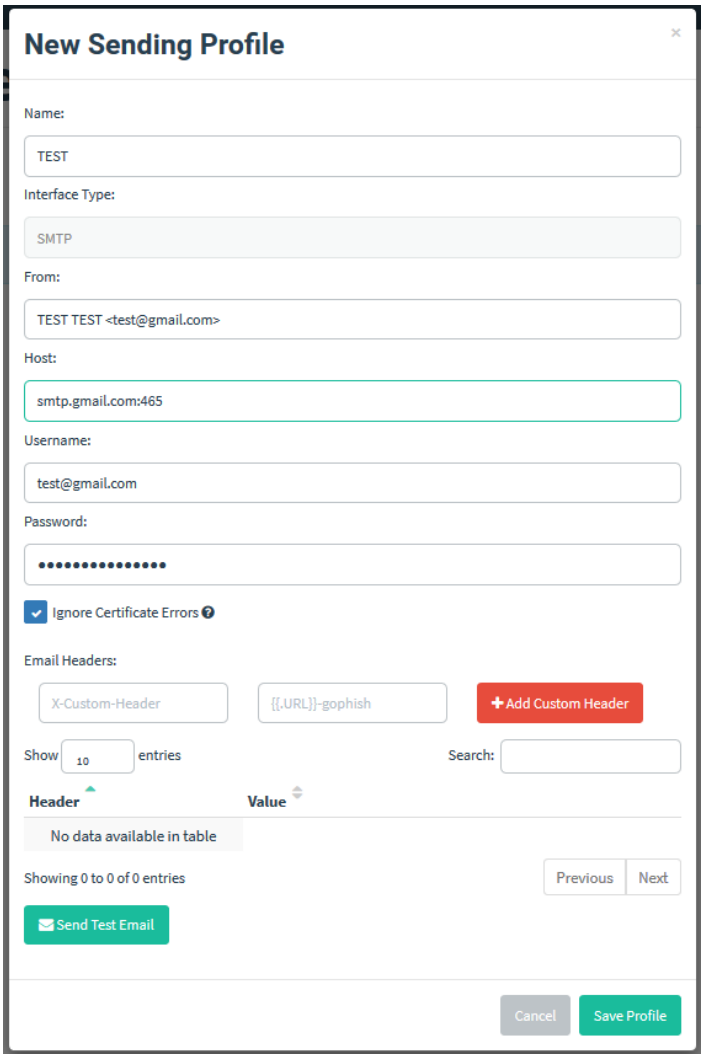
Voici le lien du dépôt Github : https://github.com/gophish/gophish

Pour cela vous allez avoir besoin de :

- VM Ubuntu avec 2GO de RAM, 60GO de Stockage & 1vCPU
- D'un serveur SMTP ou un domaine à exploiter (Un « serveur SMTP » est un serveur de messagerie qui achemine sur Internet des emails d'un expéditeur à un ou plusieurs destinataires selon les règles du protocole réseau SMTP.)

Voici un tuto YouTube au sujet de l'installation sur un environnement Linux : https://www.youtube.com/watch?v=x03fQ9JUA-E

Une fois l'installation faite, rendez-vous sur l'interface Web. Vous allez commencer par vous rendre dans l'onglet New Sending Profile pour configurer le serveur SMTP afin d'envoyer vos mails.



Name : Nom du profil,

From : Nom + adresse mail d'envoi

Host : Serveur SMTP, dépend de votre fournisseur (OVH, Gmail ...)

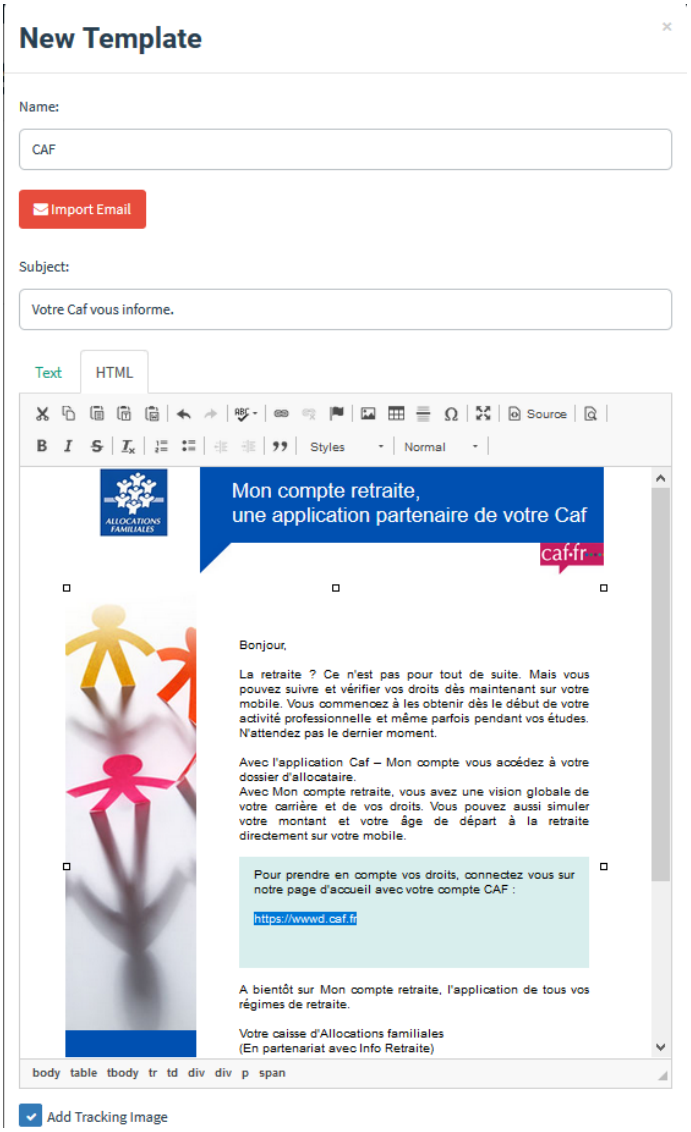
Username : Nom d'utilisateur ou mail pour se connecter au serveur SMTP

Password : Mettre mot de passe pour se connecter au serveur SMTP

Custom Header : Permet de bypass certains champs des headers de mail (X-Mailer)

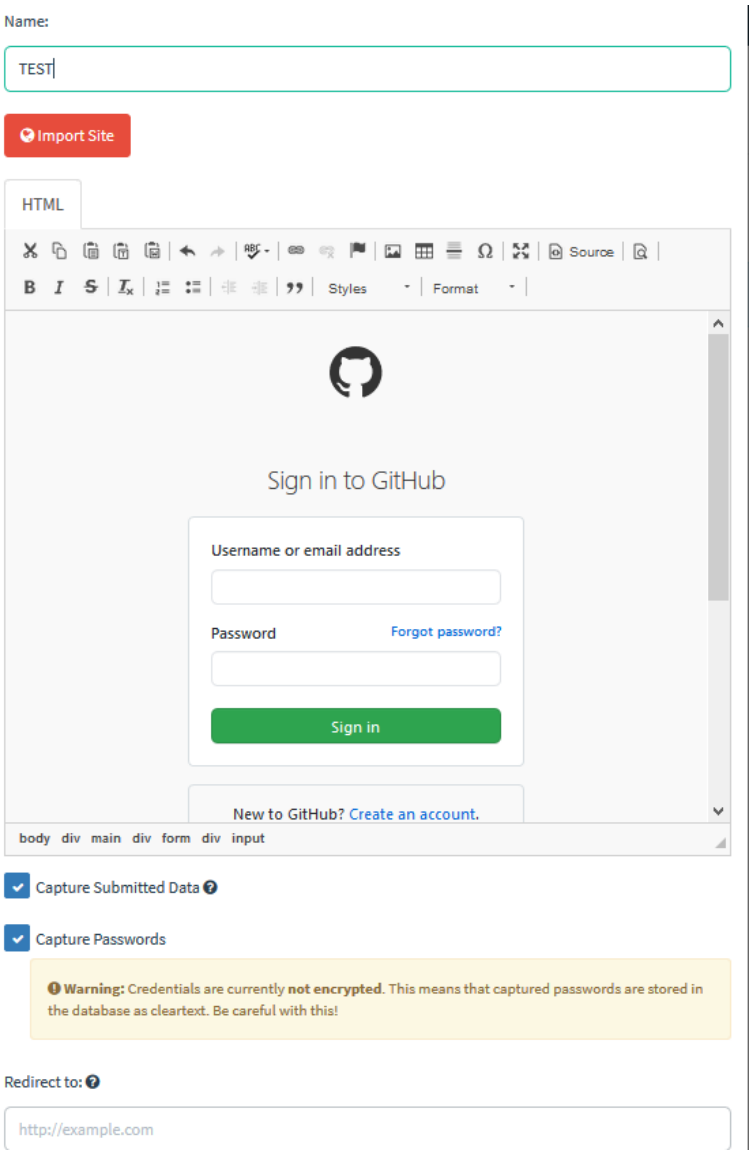
Send Test Mail : permet de savoir si la configuration est bonne.

Ensuite nous allons créer un Template de notre mail, exemple avec mail de CAF, vous pouvez **importer** un vrai mail pour rendre le vôtre plus réaliste. Pour cela, rendez-vous dans l'onglet New Template.



Dans cet exemple, j'ai mis le vrai lien de la CAF en brut, par-dessus ce texte, je vais le transformer en un lien hypertexte vers un serveur de phishing (fausse interface de connexion ou iplogger). L'option **Add Tracking Image**, permet de mettre une image transparente dans le mail, afin de savoir si l'utilisateur a ouvert le mail, si ce dernier a cliqué sur le lien, etc.

Désormais, l'onglet **Landing Pages** va nous servir à générer une fausse interface de connexion en important la page de connexion d'un site, exemple avec le site de Github :



Les options **capture submitted data** & **password** permettent de récupérer les crédentials de votre victime. L'option **Redirect to** permet de rediriger ensuite votre cible sur le vrai site pour éviter des soupçons.

Il ne nous reste plus qu'à établir la liste de nos mails cibles, pour cela rendez-vous dans l'onglet, New Group, où il ne vous reste plus qu'à créer un groupe et mettre l'ensemble des mails ou vous allez envoyer ci-dessous.

Pour finir, vous allez lancer le processus d'envoi des mails qui va marquer le début de votre campagne. Allez dans **New Campaign**, renseignez l'IP du site de la fausse interface de connexion par exemple, choisissez les différents paramètres que vous avez configurés auparavant puis lancez la campagne et attendez les résultats bien sagement sur votre Dashboard.

9 - REGEX

9.1 Explication et utilité

Une expression régulière est une séquence de caractères qui définit un modèle de recherche. Habituellement, ces modèles sont utilisés par les algorithmes de recherche de chaînes de caractères pour des opérations de "recherche" ou de "recherche et remplacement" sur les chaînes. Il s'agit d'une technique développée en informatique théorique et en théorie du langage formel.

Le concept est apparu dans les années 1950 lorsque le mathématicien américain Stephen Cole Kleene a formalisé la description d'un langage régulier. Le concept est devenu d'usage courant avec les utilitaires de traitement de texte Unix. Différentes syntaxes pour écrire des expressions régulières existent depuis les années 1980, l'une étant la norme POSIX et une autre, largement utilisée, étant la syntaxe Perl.

Les expressions régulières sont utilisées dans les moteurs de recherche, les dialogues de recherche et de remplacement des traitements de texte et des éditeurs de texte, dans les utilitaires de traitement de texte et dans l'analyse lexicale. De nombreux langages de programmation fournissent des capacités de regex soit intégrées ou via des bibliothèques.

9.2 Liste de ressources

https://regex101.com/ est un testeur de regex en ligne et un débogueur pour les langages PHP, PCRE, Python, Golang & Javascript. Il va vous permettre de comprendre comment les regex fonctionnent réellement.

http://regex.inginf.units.it/ : Cet outil est un générateur de regex.

10- SOCMINT

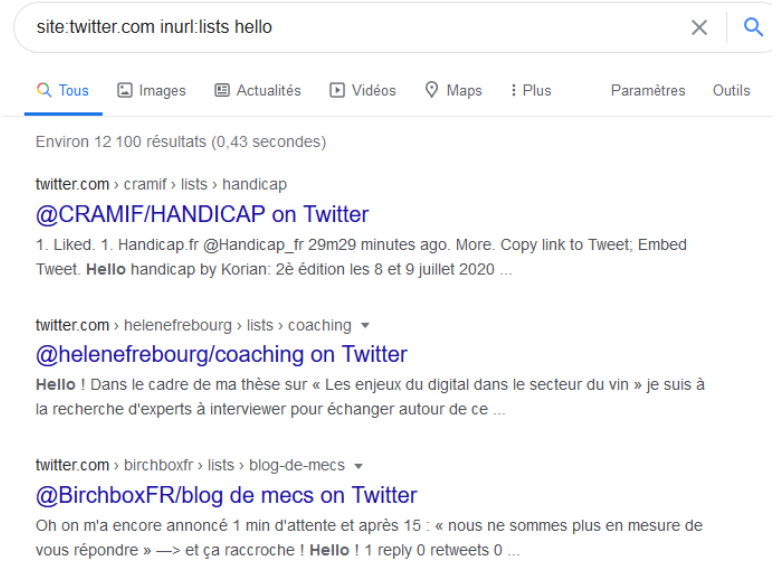
10.1 Pseudos

- **Sherlock** : Outil utile et modulable pour chercher plusieurs comptes sur des sites avec le même pseudo : https://github.com/sherlock-project/sherlock

10.2 Twitter

- **Recherche avancée :** Effectuez une recherche sur Twitter en utilisant une grande variété de filtres. Les recherches résultantes peuvent être sauvegardées, mais aussi ajustées dans la boîte de recherche ou dans l'url.

- **Google dork :** Une recherche personnalisée qui vous permet d'utiliser Google pour rechercher des listes de Twitter par mot-clé.



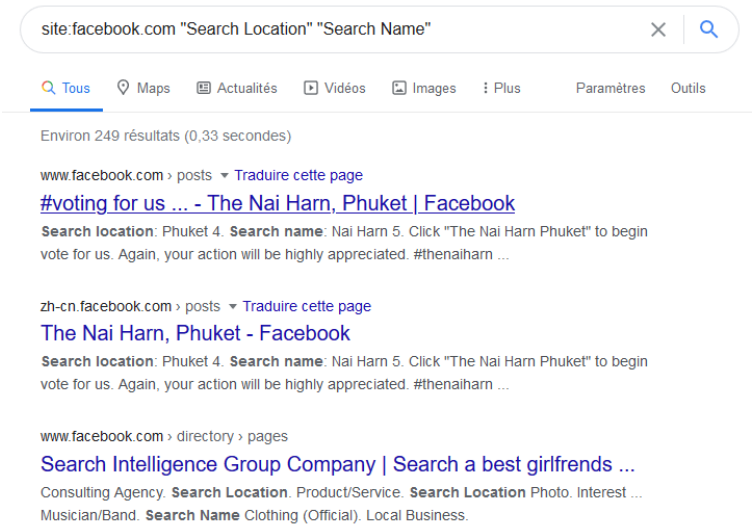
- **List_copy** : Un outil qui vous permet de copier des listes Twitter entières pour créer les vôtres : https://github.com/Noleli/listcopy
- **Spoonbill** : Suit les modifications apportées aux profils des comptes Twitter.
- **Account Analysis** : Donne des statistiques sur les comptes Twitter, temps de tweet, nombre de réponses les plus fréquentes, etc...
- **TweetBeaver** : Outil disposant d'une interface conviviale donnant une analyse des comptes, y compris pour les interactions entre les comptes.
- **TruthNest** : Outil d'analyse des comptes. Interface attrayante et conviviale et possibilité d'exporter l'analyse sous forme de fichier PDF.
- **Foller.me** : Outil d'analyse de comptes, il ne nécessite pas de se connecter à Twitter.
- **Followerwonk** : Outil d'analyse de compte. Très utile pour explorer les bios Twitter afin de trouver des comptes intéressants.
- **Twopcharts** : Analyse de comptes, suit également les tendances générales de Twitter. Offre un service plus complet pour l'abonnement payant.
- **twXplorer** : Analyse de comptes qui permet des recherches multilingues et des instantanés de résultats sauvegardés.
- **DMI-TCAT** : Ensemble d'outils permettant de récupérer et de collecter des tweets et de les analyser de différentes manières. Il est principalement écrit en PHP et fonctionne dans un environnement de serveur web :

  https://github.com/digitalmethodsinitiative/dmi-tcat/wiki

10.3 Facebook

Liste de Tools et de sites :

- **Google Dork** : De multiples dorks existent pour trouver des comptes ou données intéressantes.



- **Maltego** : Dans le cas de Facebook, Maltego propose de nombreux modules (appelés "transforms" au sein de la communauté) pour enquêter sur les profils sociaux. Les plus populaires sont les SocialLinks ou SocialNet, qui sont des modules commerciaux de Facebook OSINT.

- **Facebook ID** : Vous pouvez trouver le numéro de compte Facebook d'une personne en consultant le code source (clic droit et Afficher la source de la page) des sujets de la page Facebook et en recherchant l'expression "fb://profil/" (sans les guillemets) et le numéro de compte Facebook devrait apparaître après cela.
- **Bibliothèque de publicités Facebook** : vérifiez qui est derrière et qui dépense sur les publicités Facebook : https://www.facebook.com/ads/library/?active_status=all&ad_type=political_and_issue_ads&country=FR
- **Réinitialisation du mot de passe** : Tant que vous n'êtes pas connecté à Facebook, vous pouvez utiliser la page de réinitialisation du mot de passe pour voir si une adresse électronique ou un numéro de téléphone portable est lié à un compte Facebook actuel.

10.4 Instagram

Liste de Tools et de sites :

- **Toutatis :** Toutatis est un outil qui vous permet d'extraire des informations des comptes Instagram tels que les e-mails, les numéros de téléphone et autres : https://github.com/megadose/toutatis
- **High Resolution Downloader for Instagram** : Extension Chrome pour récupérer des images en haute résolution : https://chrome.google.com/webstore/detail/high-resolution-downloade/hbijmiokbffalbolieapplfhmmnioeao
- **Spatulah :** Scrapper pour les commentaires Instagram : https://spatulah.com/

10.5 Reddit

- **Collection de .CSV et .JSON sur de multiples informations Reddit (user, subreddits …) :** https://files.pushshift.io/reddit/
- **Archives de Reddit** : http://www.redditarchive.com/
- **Site pour analyser un utilisateur** : https://reddit-user-analyser.netlify.app/
- **Mostly Harmless :** Extension Chrome sur la recherche la page web que vous êtes en train de consulter pour voir si elle a été soumise à reddit. Si c'est le cas, vous pouvez voir partout où il a été posté, voter pour ou contre l'article, et même le sauvegarder, le cacher et le signaler directement depuis la fenêtre contextuelle. Vous pouvez même soumettre à nouveau le message à un autre sous-reddit : https://kerrick.github.io/Mostly-Harmless/#features
- **InstagramOSINT** : L'outil Instagram OSINT permet d'obtenir, à partir d'un compte Instagram, une série d'informations que vous ne pourriez normalement pas obtenir en consultant simplement son profil. Les informations comprennent : Nom d'utilisateur, Nom du profil, URL, etc… Elle intègre aussi une API pour pouvoir utiliser cela dans vos codes python. Voici le lien : https://github.com/sc1341/InstagramOSINT

10.6 Google Suite

- **GHunt** : Tool écrit en Python et qui permet d'extraire des infos sur un compte Google : https://github.com/mxrch/GHunt

10.7 LinkedIn

LinkedInt: Tool pour faire du scraping : https://github.com/vysecurity/LinkedInt

CrossLinked : Cet outil permet de simplifier les processus de recherche dans LinkedIn pour collecter les noms des employés valides lors de la vérification des mots de passe ou d'autres tests de sécurité d'une organisation : https://github.com/m8r0wn/CrossLinked

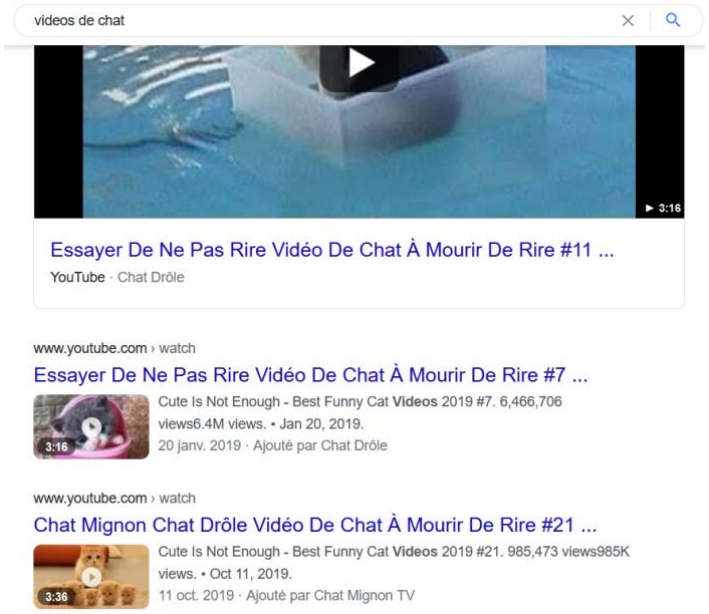
11- DORKING

11.1 Google

Les Google dorks sont des recherches sur Google avec des chaînes de recherche spécifiques qui peuvent forcer Google à renvoyer un type de résultat spécifique.

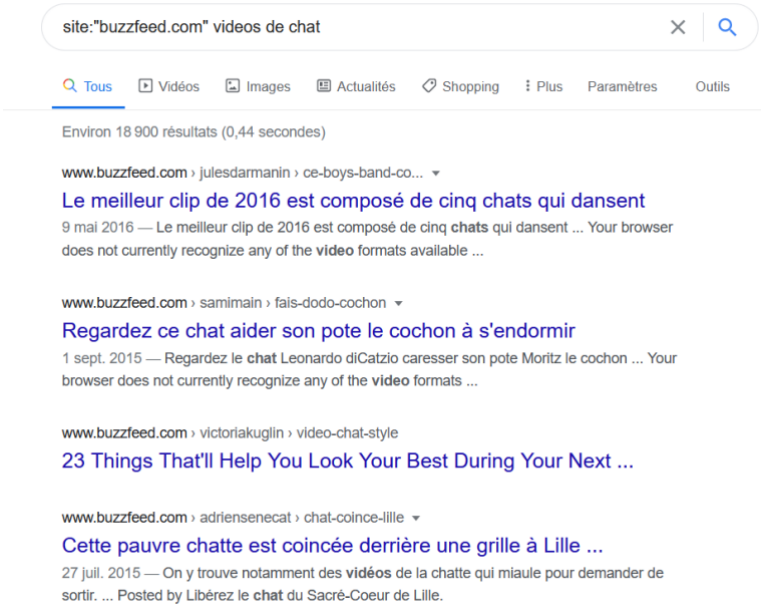
Par exemple, si vous voulez trouver des vidéos de chats uniquement sur BuzzFeed.

Mais chaque fois que vous avez cherché sur Google "vidéos de chats", la plupart des résultats étaient dominés par YouTube ou d'autres sites de partage de vidéos.



C'est là ou l'utilisation des googles dorks est pratique car maintenant nous allons chercher avec la chaîne suivante sur Google pour obtenir des résultats uniquement de Buzzfeed.

```
site :«buzzfeed.com» videos de chats
```



D'autres chaînes de caractères communes sont :

`filetype:`

`intext:`

`inurl:`

Cela permettra également de filtrer le gros des informations des sites que Google indexe et vous aidera à trouver exactement ce dont vous avez besoin. Concrètement, vous trouvez l'aiguille dans la botte de foin. Cela peut s'avérer très utile lorsqu'elle est utilisée dans le bon contexte. Si vous êtes un étudiant à la recherche de documents de recherche, par exemple.

Voici un lien avec une énorme base de données de Dork :

https://www.exploit-db.com/google-hacking-database

Si vous craignez que les moteurs de recherche indexent des parties de votre site que vous aimeriez sécuriser, vous devriez envisager d'autoriser Google à n'explorer que les parties de votre site que vous aimeriez voir indexées à l'aide d'un fichier robots.txt.

Pour en savoir plus à ce sujet : https://www.anthedesign.fr/referencement/fichier-robots-txt/

11.2 Shodan

Voici une des listes de dorks pour le site Shodan :

https://github.com/humblelad/Shodan-Dorks

https://github.com/jakejarvis/awesome-shodan-queries

Excellent tutoriel démontrant la puissance de Shodan en utilisant ce dernier avec de la créativité : https://medium.com/@Asm0d3us/weaponizing-favicon-ico-for-bugbounties-osint-and-what-not-ace3c214e139

12- INVESTIGATION EN FRANCE

12.1 Entreprise

En OSINT il peut être intéressant de s'intéresser à la partie « pro » et chercher des informations sur une personne morale plutôt que la personne physique.

Ça ne concernera pas le commun des mortels, mais dès qu'on va toucher à des personnes politique, publique il peut y avoir de la donnée à aller chercher.

Toutes les entreprises doivent publier un certain nombre d'info, et elles sont en parties publiques, mais l'accès y est souvent payant (Infogreffe).

On peut avoir des données gratuites sur des annonces légales ou autres, quelques liens ci-dessous :

https://www.pple.fr/

https://www.societe.com/

Le lien suivant, https://www.societe.ninja/ est un site très utile pour avoir des informations pouvant être payantes sur **societe.com**, Les données affichées sont fournies en OPEN DATA par des API externes :

- INSEE (Répertoire SIRENE)
- INPI (Répertoire RNCS)
- LEGIFRANCE,
- BODACC

La majorité des outils sont « pro » car utilisés par des commerciaux ou des RH. Ils proposent tous une version gratuite avec des nombres d'utilisations limitées. Pour y accéder, il faut souvent fournir une adresse mail professionnelle (avec un nom de domaine hors Yahoo, Gmail etc.).

https://hunter.io/search

Cet outil ci-dessus permet de chercher sur internet les différentes adresses mail à partir d'un nom de domaine d'adresse pro. Cela permet également de déceler la nomenclature « prénom.nom ».

12.2 Particuliers

LittleBrother est un outil de collectes d'informations qui vise à effectuer des recherches sur une personne française, suisse, luxembourgeoise ou belge. Il fournit divers modules qui permettent des recherches efficaces. LittleBrother ne requiert pas de clé API ni d'identifiant de connexion : https://github.com/lulz3xploit/LittleBrother

Operative-Framework est un Framework d'investigation numérique, vous pouvez interagir avec plusieurs cibles, exécuter plusieurs modules, créer des liens avec la cible, exporter le rapport vers un fichier PDF etc. : https://github.com/graniet/operative-framework

Conclusion

Vous êtes nombreux à me suivre sur Twitter et ce, depuis de nombreuses années.
Vous avez pu voir le nombre d'enquêtes que j'ai pu résoudre grâce à l'OSINT et au délà car oui, j'ai souvent dépassé les limites.
La « technique suprême » reste l'emprunt d'identité pour infiltrer des environnements et obtenir des informations.
@DalilBoubakeur existe depuis presque 11 ans, j'ai publié des communiqués à la place du recteur de la Gde mosquée de Paris tout en respectant sa réputation en ligne bien évidemment.

Pour être invisible en ligne, il vous faut également « emprunter » une identité qui parfois peut être réelle en copiant les données depuis un facebook ou un linkedin mais il faut veiller à ce que la personne ne possède pas de compte sur le réseau où vous souhaitez dupliquer son identité.
Sur le long terme, je vous recommande d'emprunter celle de diplomates africains ou de pays inconnus.
Sur le court terme, pour obtenir des informations sur une personne après l'avoir observée, je recommande l'emprunt de l'identité d'une personne de son second cercle : individu de la même entreprise, ami d'un ami, etc ...
Vous pourrez, comme moi, trainer sur les réseaux sociaux en étant anonymes et crédibles.

Bon courage

LC