

Sommaire

[1. Méthodologie OSINT 1](#_Toc131766163)

[2. Analyse OSINT 1](#_Toc131766164)

# 1. Méthodologie OSINT

**/ ! \ Attention : Dans l’OSINT il est important de faire attention à l’où on va chercher nos informations. Nous devons rester sur la collecte d’informations OpenSource.**

Dans une analyse OSINT il faut suivre différentes étapes :

* Méthodologie utilisée
* Outils utilisés
* Se poser des questions ouvertes

Il faut prendre en note toutes les actions effectuées sous forme de Mind Map par exemple

En OSINT il est important d’effectuer ses recherches en **«** **PIVOT »**. Une recherche en Pivot consiste à remonter petit à petit dans les informations (via un nom on retrouve un mail, via le mail on retrouve un RS, via le RS on retrouve un numéro de téléphone…)

La méthode de recherche en pivot doit être présente et visible dans un rapport

# 2. Analyse OSINT

**La 1ère analyse OSINT consiste à analyser une image :**



La 1ère recherche peut se faire via google Lens ou google image

Nous trouvons que le char est de la marque Merkava Mark 4 d’Israël. Maintenant si nous voulons plus d’informations comme le modèle du char nous pouvons analyser l’image.

Le modèle n’est un Merkava Mark 4 M & Barak. Nous pouvons le voir avec le fait que le char ne dispose pas d’un système trophy (sur la photo)

Le char dispose d’une vision panoramique non rotatif ce qui nous fait penser au modèle Merkava Mark 4 A

**La 2ème analyse OSINT consiste encore à analyser une image mais cette fois-ci plus difficile :**

Une image contenant eau, bateau, plein air, embarcation

Description générée automatiquement

A première vue il s’agit d’une Frégate Chinoise.

Avec une recherche sur google Lens nous pouvons trouver une image similaire et nous en déduisons que celle-ci a été modifiée (image retournée et floutée)

Infos sur <https://www.areion24.news/2017/01/24/interets-chinois-mer-de-chine-meridionale/>

**3ème analyse OSINT :**



Nous disposons de l’information suivante : la photo a été prise en Colombie

Nous voyons que le lieu se situe au bord de l’eau. Au loin nous voyons un bateau. Sur le bas à droite de l’image nous voyons une ligne de chemin de fer

Maintenant en utilisant google Maps nous pouvons chercher en Colombie un endroit qui correspondrait à notre image. Il est possible d’utiliser la « street view » pour retrouver les informations trouvées juste au-dessus.

Il est aussi possible d’utiliser OpenStreetMap pour trouver plus d’informations

La photo a été prise à la calle 106 au Nord de Barranquilla : 1111 calle 106, atlantico colombie

Riomar, Barranquilla, Atlántico, Colombie

**4ème Analyse : nous avons reçu le message suivant :**

籝籸 类籮籽类籲籮籿籮 籽籱籮 籸籷籮 粂籸籾 籵籸籿籮簵 粂籸籾 籶籾籼籽 籹籪粂 籽籱籮 籹类籲籬籮簷 籝籱籮 籼籾籶 籸籯 鲃簾簵簹簹簹簵簹簹簹 籶籾籼籽 籫籮 籭籮籵籲籿籮类籮籭 籽籸 籾籼 籲籷 籬籪籼籱 籽籸 籽籱籮 籵籸籬籪籽籲籸籷 籼籹籮籬籲籯籲籮籭 籲籷 籽籱籮 籯籸籵籵籸粀籲籷籰 籭籮籽籪籲籵籼 籸籯 籽籱籮 籷籸籽籮簷 籏籪籲籵籾类籮 籽籸 籭籸 籼籸 粀籲籵籵 类籮籼籾籵籽 籲籷 籭籲类籮 籬籸籷籼籮籺籾籮籷籬籮籼簷 籝籸 籹类籸籿籮 粂籸籾类 籬籸籶籶籲籽籶籮籷籽簵 类籮籪籬籱 籸籾籽 籽籸 籾籼 籿籲籪 籸籾类 籝籮籵籮籰类籪籶 籼籮类籿籲籬籮簵 簫籝籱籮籑籲籰籱籐籾籪类籭籨籋籸籽簫 籝籱籮籷 籲籷籹籾籽 籽籱籮 籼籮籬类籮籽 籼籽类籲籷籰 簫籏籸类 籢籸籾类 籎粂籮籼 籘籷籵粂簫 籪籷籭 粂籸籾 粀籲籵籵 籫籮 籰籲籿籮籷 籯籾类籽籱籮类 籲籷籼籽类籾籬籽籲籸籷籼簷 籍籸 籷籸籽 籪籽籽籮籶籹籽 籽籸 籲籷籿籸籵籿籮 籽籱籮 籪籾籽籱籸类籲籽籲籮籼 籸类 粂籸籾类 籵籸籿籮籭 籸籷籮 粀籲籵籵 籼籾籯籯籮类 籽籱籮 籬籸籷籼籮籺籾籮籷籬籮籼簷 籠籮 籪类籮 籪籵粀籪粂籼 粀籪籽籬籱籲籷籰簷 簶籝籱籮 籑籲籰籱 籐籾籪类籭簷

Traduction du message :

Dans le passé, l'entreprise a pu faire beaucoup d'appels à l'utilisation de ses propres ressources, mais elle n'a pu faire aucun appel à l'utilisation de ses propres ressources. La langue de la langue est l'anglais et la langue de la langue est l'anglais, ainsi que la langue de la langue. Le résidu du résidu du résidu du résidu est ancien et le décamètre est ancien et le résidu est ancien et le résidu est ancien et le résidu est ancien et le résidu est ancien et le résidu est ancien et le résidu est ancien et le résidu est ancien et le résidu est ancien et le résidu est ancien et le résidu est ancien et le résidu est ancien et le résidu est ancien et le résidu est ancien et le résidu est ancien.

Le message ne ressemble à rien. La traduction n’est peut-être pas nécessaire. En tapant le message sur internet nous retrouvons de l’unicode. Nous avons donc à faire à un message codé.

Nous pouvons traduire le code en allant sur le site CyberChef

Une fois sur le site nous entrons le code et nous devons le déchiffrer en ROT8000 ce qui nous donne le code suivant :

To retrieve the one you love, you must pay the price. The sum of â¬5,000,000 must be delivered to us in cash to the location specified in the following details of the note. Failure to do so will result in dire consequences. To prove your commitment, reach out to us via our Telegram service, "TheHighGuard\_Bot" Then input the secret string "For Your Eyes Only" and you will be given further instructions. Do not attempt to involve the authorities or your loved one will suffer the consequences. We are always watching. -The High Guard.

**5ème analyse : Analyse d’une image :**



Nous avons l’information que le lieu se situe du côté de Reims

A première vue l’image nous fait penser à une scierie. Afin de trouver plus facilement le lieu sur l’image nous pouvons utiliser l’outil « Overpass Turbo »

**6ème analyse : Analyse de coordonnées opérateur (Antenne) :**

Nous avons reçu par message le code suivant :

MCC: 208

MNC: 10

LAC: 12102

CID: 9448453

Ce code correspond à des coordonnées d’Antenne. Nous pouvons l’analyser avec l’outil OpenCellID <https://opencellid.org>