OSINT : Aide-Mémoire de l'Analyste (Cheat Sheet)

Ce document synthétise les concepts, outils et bonnes pratiques de la formation OSINT (Open Source Intelligence) en un guide rapide pour l'analyste.

I. Fondamentaux et Méthodologie

A. Cycle du Renseignement (Les 5 Étapes)

Étape	Objectif Principal	Résultat Clé
1. Planification	Définir la question à répondre (KIQ) et le périmètre.	Un Plan de Collecte clair.
2. Collecte	Récupérer les données brutes.	Données brutes sourcées et documentées.

Étape	Objectif Principal	Résultat Clé
3. Traitement	Transformer le bruit en information propre (Nettoyage, organisation).	Information structurée et filtrée.
4. Analyse	Mettre en relation, corroborer (vérifier) et évaluer les informations.	Renseignement actionnable (Valeur Ajoutée).
5. Diffusion	Communiquer les résultats (BLUF).	Rapport pertinent, clair et sourcé.

B. Fiabilité et Crédibilité (Grille de Fiabilité)

Les conclusions doivent se baser sur les notations A1, B1, A2, B2.

Fiabilité de la Source	Code	Crédibilité de l'Information	Code
Fiable (Registre officiel, Agence reconnue)	A	Confirmée (Corroborée par sources indép.)	1
Assez Fiable (Média de second plan)	B	Probable (Cohérente, non confirmée)	2
Peu Fiable (Source anonyme, Blog partisan)	C	Possible (Logique, pas d'autre preuve)	3

Fiabilité de la Source	Code	Crédibilité de l'Information	Code
Non Fiable (Source de désinformation)	D	Douteuse (Contredit des infos fiables)	4
Inconnue (Nouvelle source)	E	Improbable (Semble fausse)	5

C. Cadre Légal et Éthique

- **Règle d'Or :** Si vous devez contourner une mesure de sécurité, ce n'est PAS de l'OSINT (HACKING).
- **RGPD :** La collecte, le stockage et l'analyse de DCP publics sont un "traitement". Minimisez la collecte (ne collecter que le nécessaire).
- **Éthique :** Ne pas faire de *Doxing* (publication publique d'infos personnelles pour nuire). **RESTER PASSIF**.

II. Sécurité Opérationnelle (OPSEC)

L'OPSEC vise à ne pas révéler QUI vous êtes, CE QUE vous cherchez, et POURQUOI vous le cherchez.

Pilier OPSEC	Principe	Outils Clés
1. Environnement	Cloisonner l'enquête de la machine personnelle/professionnelle.	**VM** (VirtualBox, VMWare), **TAILS** (Anonymat max, amnésique), **CSI Linux** (Boîte à outils pré-installée).

Pilier OPSEC	Principe	Outils Clés
2. Connexion	Masquer l'Adresse IP.	**VPN** (No-logs), **Tor** (Anonymat très élevé, lent).
3. Identité	Utiliser une fausse identité numérique (Sock Puppet).	**ProtonMail**, **ThisPersonDoesNotExist.com** (Photo IA), Carte SIM prépayée/Service SMS en ligne, **KeePassXC** (Gestionnaire de mots de passe et de légende, hors ligne).
Protection des preuves	Chiffrer les données collectées.	**VeraCrypt** (Conteneur chiffré).

III. Outils de Collecte (L'OSINT Actif)

A. Recherche Avancée (Google Dorking)

Opérateur	Description	Exemple
`"`	Force le moteur de recherche à chercher l'expression exacte.	`"Jean Dupont"`
`-`	Exclut un mot.	`"Jean Dupont" -cycliste`

`site:`	Restreint la recherche à un domaine.	`site:[linkedin.com/in](https://linkedin.com/in) "PDG"`
`filetype:`	Recherche un type de fichier spécifique.	`filetype:pdf "rapport confidentiel"`
`inurl:`	Cherche un terme dans l'URL de la page.	`inurl:admin`
`intitle:`	Cherche un terme dans le titre de la page.	`intitle:"index of /"`
Moteurs Alternatifs :	Moteurs de recherche spécialisés ou axés sur la confidentialité.	Yandex (ROI de la recherche d'image inversée), Bing, DuckDuckGo (OPSEC).

B. Infrastructures Techniques (TECHINT)

Domaine	Objectif	Outils Clés	Pistes de Pivot
Domaines	Identifier le propriétaire (passé).	**WHOIS** (Date de création, hébergeur), **DomainTools / Whoxy** (Historique WHOIS), **ViewDNS.info** (Reverse WHOIS).	Nom/Email du propriétaire -\> Autres domaines enregistrés.
Sous-domaines	Identifier les portes de service cachées (dev, vpn, mail).	**DNS Dumpster**, **SecurityTrails** (Historique DNS).	Trouver des environnements de développement non sécurisés (ex: `dev.cible.com`).

Domaine	Objectif	Outils Clés	Pistes de Pivot
Serveurs/IP	Identifier la nature des machines connectées à Internet.	**Shodan.io / Censys** (Moteurs d'appareils), **GreyNoise** (Qualifier l'IP : bruit ou menace ?).	Trouver des webcams ouvertes, des bases de données exposées (`product:"MongoDB"`).
Archives	Retrouver du contenu supprimé.	**Wayback Machine** (archive.org), **Archive.today** (Archiver une page immédiatement).	Anciens noms d'employés, stratégies passées.
Archivage Actif	Cloner la preuve et l'analyser hors ligne.	**Wget** (Clonage de site, **OPSEC:** utiliser Tor/VPN), **Hunchly** (Archivage automatique avec preuve d'intégrité).	

C. Individus (HUMINT/SOCMINT)

Vecteur	Objectif	Outils Clés	Pistes de Pivot
Pseudo	Cartographier tous les comptes d'une cible.	**Sherlock / Maigret** (Énumération automatisée sur 300+ sites).	Nouveau pseudo trouvé -\> Nouvelle recherche sur tous les sites.

Vecteur	Objectif	Outils Clés	Pistes de Pivot
Réseaux Sociaux	Analyse comportementale (Heures, opinions, relations).	**Nitter** (Consultation X/Twitter sans se connecter - OPSEC), Google Dorks `site:linkedin.com/in "Nom Prénom"`.	Recherche par tags, commentaires (qui *like* ? qui commente ?).
Téléphone / Email	Identifier le propriétaire.	Google Dork (`"06 12 34 56 78"`), **Pages Jaunes/118 712** (France, faible efficacité mobile).	Recherche de l'email/numéro dans les brèches (HIBP, DeHashed).
Brèches de Données	Le Pivot Ultime : Lier une donnée (email, pseudo) à d'autres données (IP, mot de passe hashé).	**HaveIBeenPwned** (Email fuité ?), **DeHashed** (Contenu du leak, nécessite abonnement).	IP, Mot de passe ou Pseudo trouvé -\> TECHINT ou HUMINT.

D. Images (IMINT/VIDINT)

Outil/Technique	Objectif	Usage OSINT
Recherche Inversée	Trouver l'origine, la date de première apparition, d'autres versions.	**Yandex** (Meilleur pour les visages/lieux), **Google Images**, **TinEye** (Meilleur pour l'historique), **Bing Visual Search**.

Outil/Technique	Objectif	Usage OSINT
Métadonnées (EXIF)	Lire l'heure, l'appareil, le logiciel, les coordonnées GPS (si non supprimées).	**ExifTool** (Professionnel), exif.tools (En ligne).
Géolocalisation	Trouver un lieu SANS GPS.	Indices visuels (Langue, architecture, végétation). **Google Maps/Street View**, **Google Earth Pro** (Images historiques, 3D), **SunCalc.net** (Estimer l'heure/l'orientation).

E. Documents Spécifiques (DOC-INT)

Technique	Description	Outils
Extraction de Métadonnées	Auteur, nom de l'entreprise, chemins de serveurs cachés dans PDF/DOCX/XLSX.	**ExifTool**, **Metagoofil** (Automatisation de la recherche et de l'extraction).
Analyse Fichiers	Chercher les commentaires cachés, les révisions (Word), les lignes masquées (Excel).	Logiciel de bureau (Word, Excel, etc.) ou visionneuse spécialisée.

Technique	Description	Outils
OCR	Rendre le texte d'une image (PDF image, JPG) interrogeable.	**Google Lens**, **Yandex** (Clic droit sur image), **Tesseract**.

IV. Outils de Production et d'Organisation

Catégorie	Outil	Fonction Clé
Mind Mapping	**XMind**	Structurer la Planification, les KIQ et les pistes.
Notes / Centralisation	**Obsidian** (Local, OPSEC), **Notion**	Créer le "Cahier d'Enquête Numérique", lier les notes.
Veille Passive	**Google Alerts**, **Feeds RSS**	Laisser l'information venir à vous sur mots-clés ou URL spécifiques.
Analyse de Liens	**Maltego**, **Lampyre**	Visualiser les relations entre les données (Personne -\> Email -\> IP -\> Domaine).

Catégorie	Outil	Fonction Clé
Intégrité de la Preuve	**Hunchly**	Archiver chaque page avec une signature cryptographique (hachage) pour la recevabilité légale.