**OSINT COMME OUTIL D'ENQUÊTE**

MÉTHODOLOGIE D'ENQUÊTE

Qu'est-ce que la méthodologie d'enquête ?

* La méthodologie d'enquête est un ensemble structuré de méthodes reproductibles permettant de transformer des outils et des données brutes en conclusions fiables, et sans une méthode reproductible, l'OSINT reste une collection d'outils sans rigueur.
* Elle vise à formaliser les étapes de collecte, de vérification et d'interprétation des données pour assurer la traçabilité et la défendabilité des résultats en contexte judiciaire ou opérationnel.

Évolution depuis Sherlock Holmes

* Les principes classiques d'observation et de déduction sont toujours pertinents, mais ils doivent être adaptés aux volumes et à la nature numérique des données actuelles.
* L'évolution implique l'intégration de techniques scientifiques, de datation chronologique et de comparaison systématique des preuves numériques pour éviter les biais d'interprétation.

Méthodes d'enquête et traduction au numérique

* Les méthodes d'enquête incluent l'observation, l'interrogation, la chronologie, la baseline et l'analyse médico-légale, qui se traduisent en OSINT par la capture d'artefacts numériques, la vérification des métadonnées et l'analyse comparative de sources.
* Les techniques numériques exigent des outils spécifiques pour la collecte, la conservation et la visualisation des preuves, ainsi qu'une attention particulière à la reproductibilité et à la rétention des données.

COMPTE RENDU DE TÉMOIN

Qui est un témoin et combien doivent être interrogés

* Un témoin est toute personne ayant vu, entendu ou possédant une information pertinente à l'enquête, et l'approche recommande d'interroger plusieurs témoins pour trianguler les informations et réduire les erreurs de perception.
* Multiplier les entretiens augmente la capacité à identifier des contradictions, des recoupements et des éléments confirmant la chronologie ou les motifs.

Comportement cognitif et indicateurs non verbaux

* L'analyse du comportement cognitif et des indices non verbaux doit aider à évaluer la crédibilité, car des hesitations, des incohérences ou des signaux non verbaux peuvent indiquer omission, manipulation ou stress.
* En OSINT, ces indices se transposent par l'examen des patterns linguistiques, des variations temporelles dans les publications et des changements comportementaux sur les comptes en ligne.

Schémas de parole et manipulation du temps

* Les patterns de discours, comme l'utilisation répétée de formulations vagues ou l'ajout excessif de détails, sont des signaux d'alerte qui aident à évaluer la fiabilité d'un témoignage.
* La manipulation temporelle (retards, imprécisions ou modifications d'horodatages) doit être cherchée et vérifiée par recoupement avec d'autres sources et métadonnées.

Manque de détail et surcompensation

* Un manque de détails précis peut indiquer une mémoire défaillante ou une tentative d'omission, tandis qu'une surabondance de détails peut être une stratégie de crédibilité; ces deux extrêmes nécessitent vérification.
* L'analyse de déclaration et le croisement avec d'autres témoins ou données permettent d'identifier quelles informations sont corroborées et lesquelles doivent être suspectées.

Analyse des déclarations et recherche de témoins supplémentaires

* L'analyse des déclarations implique une désagrégation systématique des affirmations pour en vérifier chaque élément par des sources externes ou des preuves matérielles.
* Trouver des témoins supplémentaires et des données de soutien (photos, vidéos, logs) augmente la robustesse des conclusions et permet de reconstituer des événements avec plus de précision.

CHRONOLOGIE

Établir un point fixe et étendre la ligne temporelle

* Il faut d'abord définir un point fixe vérifiable (horodatage, événement corroboré) à partir duquel construire la chronologie et ensuite étirer la ligne temporelle aussi largement que nécessaire pour capturer le contexte.
* L'élargissement de la période permet d'identifier des précurseurs ou des conséquences qui pourraient être essentiels à la compréhension de l'incident.

Tableaux des faits et de l'information

* Créer un tableau des faits (éléments vérifiés) et un tableau d'information (données à vérifier) permet de déplacer les éléments entre ces tableaux au fur et à mesure de leur validation.
* Cette séparation aide à formaliser le travail de vérification et à clairement documenter l'état de chaque élément de preuve.

Vérification, données auxiliaires et interrogation des lacunes

* La vérification doit rechercher quelles autres sources peuvent appuyer un fait, et un fait confirmé peut mener à la découverte d'autres données connexes ou auxiliaires.
* Il est essentiel d'analyser minute par minute les périodes couvertes, d'identifier les lacunes et de formuler des hypothèses sur ce qui a pu se passer avant et après ces plages temporelles.

Questionnement des inexactitudes et recoupement des données

* Les inexactitudes déclarées doivent être interrogées, confirmées ou mises en suspicion, et toutes les données doivent systématiquement être recoupées pour assurer leur fiabilité.
* Le recoupement inclut la mise en relation de métadonnées, de captures d'écran, de logs réseau et d'autres sources indépendantes.

RÉFÉRENCE DE BASE (BASELINE)

Importance de la mesure et de la comparaison

* Sans possibilité de mesurer un état de référence, il est impossible de gérer et d'identifier des anomalies; la baseline permet de déceler des variations significatives.
* La constitution d'une baseline consiste à collecter des données représentatives dans des conditions normales pour pouvoir détecter ultérieurement des écarts ou des comportements anormaux.

Principe de Locard et analyse comparative

* Le principe de Locard (transfert de traces) s'applique au numérique en recherchant des micro-traces laissées par des acteurs, et l'analyse comparative permet de lier des artefacts entre eux.
* L'analyse comparative utilise des métriques et des indicateurs techniques pour établir des similarités ou des différences entre jeux de données.

EXAMEN MÉDICO-LÉGAL (FORENSIQUE)

Focalisation sur les faits et absence de conclusion prématurée

* L'approche médico-légale se concentre strictement sur les faits observables et consignés, et il est fréquent qu'aucune conclusion définitive ne soit atteinte sans preuve supplémentaire.
* Les investigations médico-légales insistent sur la neutralité, la traçabilité et la documentation rigoureuse de chaque étape d'analyse.

Substantiation, établissement d'éléments manquants et création de liens

* La forensique vise à substancier les allégations, à identifier et combler des éléments manquants et à créer des liens entre diverses sources de données.
* Cela implique souvent l'utilisation de sciences exactes, de mathématiques et de méthodes de data science pour objectiver les preuves.

Attention méticuleuse aux détails et usage scientifique

* Une attention scrupuleuse aux détails est requise, incluant l'examen des métadonnées, des fragments d'information et des artefacts discrets.
* L'utilisation de méthodes scientifiques et d'outils statistiques aide à valider des hypothèses et à quantifier la confiance dans les résultats.

APPLICATION DES MÉTHODES À L'OSINT

Définition claire du périmètre et identification des couches de données

* Il est essentiel de définir précisément le périmètre de travail, d'identifier la couche de données (surface web, réseaux sociaux, données d'infrastructure, etc.) la plus susceptible de contenir la preuve recherchée.
* Une délimitation claire du scope évite la dispersion des efforts et oriente le choix des outils et des techniques.

Sélection d'outils, conduite de la recherche et analyse

* Après avoir identifié la couche pertinente, il faut choisir les outils appropriés pour acquérir les données, conduire la recherche, puis analyser ces données pour en évaluer la précision et l'interprétation.
* L'analyse doit inclure l'évaluation critique des sources, la validation croisée et la prise en compte d'alternatives interprétatives.

Capturer les résultats et produire des conclusions factuelles

* Les résultats doivent être capturés selon une méthode acceptée en cour, en documentant la chaîne de conservation et la reproductibilité.
* Les conclusions présentées doivent être concises, factuelles et limitées aux éléments effectivement prouvés par les données.

ADÉQUATION ET SÉLECTION DES OUTILS

Critères de sélection : adapté à l'objectif et rétention des données

* Les outils doivent être choisis en fonction de leur adéquation à la tâche (fit to purpose) et en tenant compte de la politique de rétention des données si l'outil est en ligne.
* La rétention des données influence la capacité à récupérer des preuves historisées et la reproductibilité des résultats.

Comportement d'enquêteur, exactitude et disponibilité

* L'usage répété d'un même outil peut laisser des empreintes procédurales; il faut donc varier les approches et documenter les choix méthodologiques.
* L'exactitude des résultats, l'existence d'alternatives et la disponibilité (coût, accès, restrictions) sont des facteurs clés dans la sélection d'un outil.

MÉTHODE MINIMALE

Gestion du flux de travail avec des gestionnaires de favoris

* Utiliser des gestionnaires de favoris ou de bookmarks permet de contrôler le flux de travail, de conserver des sources et de retrouver facilement les étapes de la recherche.
* Cette pratique soutient la reproductibilité et la constance des résultats entre différentes sessions d'enquête.

Reproductibilité comme condition de cohérence

* Si les résultats ne peuvent pas être reproduits, il est impossible d'assurer la cohérence et la fiabilité des produits d'enquête; la méthode minimale impose des étapes obligatoires pour garantir la répétabilité.
* La standardisation des processus et l'utilisation d'outils qui enregistrent les actions contribuent à cette reproductibilité.

LATCHES ET PIVOTS

Concept général et utilité

* Les "latches" (points d'ancrage) et les "pivots" (mouvements de focalisation entre sources) servent à structurer la navigation entre indices et à étendre une enquête à partir d'un artefact initial.
* Ils permettent d'identifier des connexions opérationnelles entre comptes, numéros, images et autres entités en passant d'une source à une autre de façon méthodique.

Application pratique en OSINT

* En pratique, cela implique d'utiliser un élément vérifié (par ex. un numéro de téléphone ou une photo) comme point d'ancrage pour découvrir d'autres artefacts liés via recherche inversée, métadonnées ou corrélations temporelles.
* Les pivots doivent être documentés pour conserver la chaîne d'investigation et pour permettre la revue indépendante de la logique de connexion.

VISUALISATION

Liste des sources et plateformes à visualiser

* Les plateformes et sources listées incluent Facebook, TikTok, TrueCaller, données de fuite, LinkedIn, Uber, Telegram, Surface Web, WhatsApp, Instagram, RocketReach, CRDB Porting, données de crédit, HLR/VLR, PhoneInfoga, Mr Delivery, Spokeo et Waze, chacune nécessitant des techniques spécifiques de collecte et d'interprétation.
* Visualiser les relations entre ces sources aide à déceler des patterns d'activité, des réseaux de comptes et des corrélations géospatiales ou temporelles.

Rôle de la visualisation dans l'analyse

* La visualisation permet de transformer des relations complexes entre entités en représentations compréhensibles, facilitant l'identification de clusters, de centralités et d'anomalies.
* Elle sert aussi à communiquer clairement les conclusions aux parties prenantes non techniques, en montrant le lien entre données brutes et inférences.

Z-SEARCH PHOTOS

Usage et exemples

* La méthode Z-Search pour les photos consiste à utiliser des recherches inversées d'images et des techniques d'analyse d'artefacts visuels pour relier une image à des comptes, des lieux et des moments spécifiques.
* Des exemples pratiques incluent la recherche d'un compte TikTok spécifique (par ex. le lien fourni vers @the\_josemonkey) pour extraire des images et métadonnées pertinentes.

Importance pour l'investigation

* L'analyse d'images peut révéler des signatures uniques (objets, arrière-plans, métadonnées) qui servent de latches pour poursuivre l'investigation vers d'autres ressources numériques.
* La documentation des résultats et l'utilisation d'outils spécialisés renforcent la valeur probante des découvertes visuelles.

VLC POUR LE DÉCOUPAGE D'IMAGE (IMAGE SLICING)

Méthode et utilité

* L'utilisation de VLC Player pour découper des vidéos en tranches facilite l'analyse image par image et permet d'isoler frames pertinents pour examen et recherche inversée.
* Le découpage en segments et la sauvegarde des images extraites permet d'analyser les métadonnées et de créer des éléments vérifiables à intégrer dans la chronologie.

Application technique

* Réduire des vidéos en slices aide à repérer des détails fugitifs (numéros, plaques, logos) et à synchroniser des événements sur la timeline, ce qui est critique pour la reconstitution factuelle.
* Les images extraites doivent être conservées avec les informations sur l'origine du fichier et l'horodatage pour maintenir la chaîne de preuve.

APPLICATION PRATIQUE

Portée, plan et identification des données nécessaires

* Un plan d'enquête OSINT doit commencer par l'identification précise des données nécessaires, déterminer sur quelle couche ces données sont susceptibles d'exister et lister les outils possibles pour les acquérir.
* Il faut aussi définir des outils alternatifs et prévoir une stratégie si une source devient indisponible.

Méthodologie, technique et méthode minimale

* Adopter une méthodologie définie, appliquer des techniques comme la visualisation et le lien entre sources, et s'en tenir à sa méthode minimale pour garantir reproductibilité et cohérence.
* Utiliser des outils pour faire respecter la méthode, réduire les vidéos en slices pour l'analyse et appliquer la méthode Z-Search pour travailler les images.

Visualisation, liaison et spécificités d'image

* Visualiser et lier les éléments de recherche permet d'identifier des patterns et de construire des narratifs basés sur des preuves vérifiées; l'accent est mis sur la réduction des médias en éléments analysables.
* Pour les images, la méthode Z-Search est recommandée pour relier visuels et entités, et toutes les étapes doivent être documentées pour une utilisation légale ou opérationnelle.

CITATION ET CONCLUSION

Réaffirmation de la nécessité d'une méthode reproductible

* La citation répétée souligne que sans une méthode d'enquête reproductible, l'OSINT ne constitue qu'une collection d'outils attrayants mais peu fiables, et la reproductibilité est présentée comme la pierre angulaire d'une pratique OSINT sérieuse.
* Cette idée conclut le document en rappelant que le cadre méthodologique, la documentation et la conservation des preuves sont essentiels pour intégrer des TTP OSINT dans un framework structuré similaire à MITRE ATT&CK.

**To-Do List Version :**

1. **Définir l’objectif et le périmètre**

* **Énoncer clairement la question d’investigation et les livrables attendus.**
* **Délimiter la portée temporelle, géographique et thématique.**
* **Identifier les contraintes juridiques, de confidentialité et d’éthique.**

1. **Mettre en place la méthodologie reproductible**

* **Documenter la méthode d’enquête (étapes, critères de vérification).**
* **Mettre en place un système de versioning pour les notes et preuves.**
* **Standardiser les formats de capture (captures d’écran, métadonnées, exports).**

1. **Organiser l’environnement de travail**

* **Créer un espace de travail structuré (répertoires, noms de fichiers, templates).**
* **Configurer des outils de gestion de signets/bookmarks pour tracer le workflow.**
* **Noter les outils et les versions utilisés pour chaque tâche.**

1. **Collecte initiale et cartographie des sources**

* **Identifier les couches de données prioritaires (sources primaires vs secondaires).**
* **Lister les comptes, sites, bases de données et archives à consulter.**
* **Relever les informations d’identification et de rétention de chaque source.**

1. **Établir le baseline (bases de comparaison)**

* **Définir et documenter les points de référence mesurables (habitudes, horaires, formats).**
* **Collecter données de référence pour comparer changements ou anomalies.**
* **Noter les limites et marges d’erreur attendues.**

1. **Gestion des témoins et recueil de déclarations**

* **Déterminer qui est témoin pertinent et estimer le nombre d’entretiens nécessaires.**
* **Préparer questions structurées et critères d’évaluation des réponses.**
* **Observer et noter indices cognitifs, non-verbaux et patterns de langage.**
* **Chercher témoins corroborants et enregistrer leurs relations et biais possibles.**

1. **Construction et vérification de la timeline**

* **Choisir un point de référence fixe (UTC/date/événement) et l’appliquer partout.**
* **Rassembler tous les éléments datés et les placer sur une timeline large.**
* **Séparer « faits vérifiés » et « informations non vérifiées » ; déplacer au fur et à mesure de la vérification.**
* **Analyser les trous temporels et rechercher données annexes (logs, metadata).**

1. **Collecte et conservation des preuves**

* **Capturer preuves avec métadonnées complètes (horodatage, URL, méthode de capture).**
* **Utiliser formats exportables et acceptés légalement (PDF certifié, CSV, captures horodatées).**
* **Conserver copies immuables et journaux d’accès (hash, checksum si possible).**

1. **Analyse factuelle et forensique**

* **Croiser sources et construire liens (cartographie relationnelle).**
* **Appliquer raisonnement scientifique : hypothèses, tests, rejet des hypothèses non soutenues.**
* **Utiliser méthodes mathématiques/statistiques et outils de data science si pertinent.**
* **Documenter incertitudes et niveaux de confiance sur chaque élément.**

1. **Triangulation et corroboration**

* **Rechercher preuves alternatives pour chaque élément clé.**
* **Prioriser corroboration par sources indépendantes et hétérogènes.**
* **Noter contradictions et plan d’investigation pour les résoudre.**

1. **Choix des outils et évaluation continue**

* **Pour chaque outil, documenter : stockage/retention, biais connus, limites d’accès, coût.**
* **Préférer outils adaptés au besoin (fit-for-purpose), prévoir alternatives.**
* **Mettre à jour la liste d’outils et retester régulièrement.**

1. **Rédaction et formatage des livrables**

* **Rédiger conclusions courtes, factuelles et sourcées.**
* **Inclure timelines, résumés des preuves et annexes (captures, logs, hash).**
* **Fournir un journal d’audit détaillant étapes et reproductions possibles.**

1. **Assurance qualité et reproductibilité**

* **Demander qu’un pair reproduise une partie critique de l’enquête à partir des notes.**
* **Corriger les lacunes méthodologiques identifiées.**
* **Maintenir checklist de conformité (captures, métadonnées, export, journalisation).**

1. **Gestion des risques et confidentialité**

* **Évaluer risques opérationnels et juridiques avant diffusion.**
* **Anonymiser si nécessaire et limiter les partages aux destinataires autorisés.**
* **Archiver les preuves selon procédure de conservation.**

1. **Boucle d’apprentissage et amélioration continue**

* **Tenir un retour d’expérience après chaque enquête (ce qui a fonctionné / non).**
* **Mettre à jour templates, listes d’outils et méthodologies.**
* **Former les collègues aux bonnes pratiques et à la reproductibilité.**

**Checklist finale avant clôture**

* **Objectifs et périmètre définis et documentés.**
* **Toutes les preuves capturées avec métadonnées et copies immuables.**
* **Timeline construite et séparée en faits vérifiés / informations.**
* **Sources triangulées et les limites clairement indiquées.**
* **Méthode et workflow suffisamment documentés pour réplication.**
* **Livrable rédigé, sourcé et prêt pour usage légal si nécessaire.**