[LEXIQUE ULTIME : INVESTIGATION & CRIMINALISTIQUE]

RÉFÉRENCE : LEX-SENTINELLE-2026-V1
USAGE : FORMATION CONTINUE / CONCOURS PTS
STATUT : DIFFUSION LIBRE

PÔLE 01 : LES ACTEURS ET LES STRUCTURES

- PTS (Police Technique et Scientifique) : Ensemble des services de police chargés de la recherche et de l'identification des auteurs d'infractions.
- LPS (Laboratoire de Police Scientifique) : Structure où sont réalisées les analyses complexes (biologie, toxicologie, informatique).
- SLPT (Service Local de Police Technique) : Unité de proximité gérant les scènes de crime du quotidien (cambriolages, dégradations).
- SRIJ (Service Régional de l'Identité Judiciaire) : Unité de niveau régional pour les scènes de crime complexes.
- IRCGN (Institut de Recherche Criminelle de la Gendarmerie Nationale) : L'équivalent de la police scientifique, mais pour la Gendarmerie (Pôle d'excellence à Pontoise).
- ICC (Investigateur en Cybercriminalité) : Technicien de terrain formé à la saisie de matériel informatique et aux premières constatations numériques.
- N-TECH (Enquêteur Technologies Numériques) : L'équivalent de l'ICC chez les Gendarmes.
- C3N (Centre de Lutte contre les Criminalités Numériques) : Unité d'élite de la Gendarmerie pour les cyberattaques massives.
- OCLCTIC (Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication) : Le "FBI" français du cyber.

PÔLE 02 : CRIMINALISTIQUE DE TERRAIN ET PREUVE (LA SCÈNE DE CRIME)

- SCELLÉ : Objet saisi lors d'une perquisition, placé sous emballage sécurisé pour garantir son intégrité physique.

[LEXIQUE ULTIME : INVESTIGATION & CRIMINALISTIQUE]

RÉFÉRENCE : LEX-SENTINELLE-2026-V1
USAGE : FORMATION CONTINUE / CONCOURS PTS
STATUT : DIFFUSION LIBRE

- CHAÎNE DE POSSESSION (Chain of Custody) : Document traçant chaque intervenant ayant manipulé le scellé depuis sa saisie jusqu'au tribunal.
- GEL DES LIEUX : Opération consistant à sécuriser une scène de crime pour empêcher toute pollution des indices.
- TRANSVERSE (Traces) : Échanges de matières entre l'auteur, la victime et le lieu (Principe de Locard : "Tout individu, dans un lieu, laisse une trace et emporte une trace").
- RÉVÉLATEUR (Dactyloscopie) : Produit chimique (poudre, cyanoacrylate, ninhydrine) utilisé pour faire apparaître des empreintes digitales invisibles (traces latentes).
- SIGNALÉTIQUE : Opération consistant à relever les empreintes, photos et ADN d'un gardé à vue (Fichier FAED et FNAEG).
- DACTYLOSCOPIE : L'étude des empreintes digitales.

Adermatoglyphie : Absence rare d'empreintes.
Minuties : Points caractéristiques (arrêts, bifurcations) qui rendent l'empreinte unique. Il en faut 12 points en France pour une identification formelle.

- BIOLOGIE (ADN) : FNAEG : Fichier National Automatisé des Empreintes Génétiques.

Trace de contact : ADN laissé par simple toucher (cellules épithéliales).
Trace biologique : Sang, salive, sperme (contient plus d'ADN).

- LUMINOL / BLUESTAR : Produits chimiques qui font réagir l'hémoglobine et révèlent des traces de sang lavées ou invisibles, même des années après.
- BALISTIQUE : Étude des armes, munitions et trajectoires.

Stries de canon : Chaque arme raye la balle de façon unique, comme une empreinte digitale.
GSR (Gunshot Residue) : Résidus de tir sur les mains ou vêtements du tireur.

- ODONTOLOGIE LÉGALE : Identification par la denture (très utile sur les corps brûlés).

[LEXIQUE ULTIME : INVESTIGATION & CRIMINALISTIQUE]

RÉFÉRENCE : LEX-SENTINELLE-2026-V1
USAGE : FORMATION CONTINUE / CONCOURS PTS
STATUT : DIFFUSION LIBRE

PÔLE 03 : DIGITAL FORENSICS (L'AUTOPSIE NUMÉRIQUE)

- IMAGE BIT-À-BIT (Physical Image) : Copie exacte d'un support de stockage, secteur par secteur, incluant l'espace non alloué et les fichiers supprimés.
- HASH (SHA-256 / MD5) : Valeur mathématique unique (empreinte) d'un fichier. Si une seule donnée change, le hash change.
- CARVING (Data Carving) : Technique consistant à chercher des en-têtes de fichiers (Magic Bytes) directement dans les données brutes pour reconstruire des fichiers supprimés.
- SLACK SPACE (Espace perdu) : Espace restant dans un secteur de disque après l'écriture d'un fichier, où des données anciennes ou cachées peuvent subsister.
- ARTEFACT : Trace numérique laissée par l'utilisation d'un logiciel ou d'un système (ex: historique de recherche, fichiers récents, Prefetch).
- COLD BOOT ATTACK : Technique permettant de récupérer les clés de chiffrement restées en mémoire vive (RAM) juste après l'extinction d'un PC.
- LIVE FORENSICS : Analyse d'un système pendant qu'il est encore allumé (capture de RAM, connexions réseaux actives).
- ESPACE NON ALLOUÉ (Unallocated Space) : Zones du disque dur qui ne contiennent pas de fichiers actifs mais où résident les données supprimées non encore écrasées.
- IMAGE PHYSIQUE vs LOGIQUE : * Physique : Copie de tout le support (bit-à-bit), y compris le vide.

Logique : Copie seulement des fichiers visibles par l'utilisateur.

- STÉGANOGRAPHIE : Art de cacher un message ou un fichier à l'intérieur d'un autre (ex: un texte caché dans les pixels d'une photo de chat).
- METADATA (EXIF / IPTC) : Données cachées dans les fichiers. Pour une photo : modèle du capteur, focale, date exacte et souvent coordonnées GPS.

[LEXIQUE ULTIME : INVESTIGATION & CRIMINALISTIQUE]

RÉFÉRENCE : LEX-SENTINELLE-2026-V1
USAGE : FORMATION CONTINUE / CONCOURS PTS
STATUT : DIFFUSION LIBRE

- PERSISTANCE : Capacité d'un malware ou d'un outil de traque à rester actif même après un redémarrage (via le Registre Windows ou des tâches planifiées).
- RAM DUMP : Capture de la mémoire vive avant d'éteindre le PC pour récupérer des mots de passe en clair ou des conversations cryptées.

PARTIE 04 : LES FONDATIONS JURIDIQUES

- APJ / OPJ : Agent / Officier de Police Judiciaire. L'OPJ dirige l'enquête, l'APJ le seconde. En PTS, tu es souvent sous les ordres d'un OPJ.
- FLAGRANT DÉLIT (Art. 53 CPP) : Enquête ouverte lorsqu'un crime ou délit est en train de se commettre ou vient de se commettre. Permet des perquisitions sans l'accord de la personne.
- ENQUÊTE PRÉLIMINAIRE (Art. 75 CPP) : Cadre classique. Nécessite l'assentiment manuscrit de la personne pour perquisitionner son domicile ou son matériel.
- COMMISSION ROGATOIRE (CR) : Mandat donné par un Juge d'Instruction à un enquêteur pour effectuer des actes précis (écoutes, perquisitions complexes).
- RÉQUISITION : Ordre écrit donné à un expert ou un organisme (ex: Orange, Google) pour fournir des données ou une analyse.
- VICE DE PROCÉDURE : Erreur technique ou juridique qui rend un acte (ou toute l'enquête) nul et non avenu.

PARTIE 05 : RENSEIGNEMENT ET ANALYSE

- OSINT (Open Source Intelligence) : Renseignement d'origine sources ouvertes. Utilisation de données publiques pour enquêter.
- IMINT (Image Intelligence) : Analyse de photos et d'images satellites pour géolocaliser ou identifier des objets/personnes.

[LEXIQUE ULTIME : INVESTIGATION & CRIMINALISTIQUE]

RÉFÉRENCE : LEX-SENTINELLE-2026-V1
USAGE : FORMATION CONTINUE / CONCOURS PTS
STATUT : DIFFUSION LIBRE

- GEOINT (Geospatial Intelligence) : Renseignement basé sur l'exploitation des données géographiques.
- SOCMINT (Social Media Intelligence) : Analyse spécifique des données provenant des réseaux sociaux.
- ANACRIM (Analyse Criminelle) : Méthodologie utilisant des logiciels de visualisation (comme IBM i2 Analysts Notebook) pour croiser des flux financiers, des appels téléphoniques et des emplois du temps.
- DARKNET / DEEP WEB : Le Deep Web est la partie non indexée du web. Le Darknet est une partie du Deep Web accessible uniquement via des protocoles spécifiques (Tor, I2P) garantissant l'anonymat.
- DORKS (Google Hacking) : Utilisation d'opérateurs de recherche avancés (ex: *filetype:pdf "confidentiel"*) pour trouver des documents cachés.
- WHOIS : Protocole permettant de savoir à qui appartient un nom de domaine (site web) et où il est hébergé.
- WAYBACK MACHINE : Archive du web permettant de voir des versions passées de sites internet, même s'ils ont été supprimés.
- SCRAPING : Extraction automatisée de données d'un site web ou d'un réseau social via des scripts (Python).
- PIPL / EYESHARE : Outils de recherche de personnes croisant mails, pseudos et numéros de téléphone.

PARTIE 05 : CYBERSÉCURITÉ ET OPSEC

- OPSEC (Operational Security) : Processus visant à protéger ses propres traces pour éviter d'être identifié par l'adversaire lors d'une enquête.
- VULNÉRABILITÉ 0-DAY : Faille informatique de sécurité n'ayant pas encore de correctif connu.
- INGÉNIERIE SOCIALE (Social Engineering) : Art de manipuler des personnes pour obtenir des informations confidentielles ou l'accès à un système.

[LEXIQUE ULTIME : INVESTIGATION & CRIMINALISTIQUE]

RÉFÉRENCE : LEX-SENTINELLE-2026-V1
USAGE : FORMATION CONTINUE / CONCOURS PTS
STATUT : DIFFUSION LIBRE

- CHIFFREMENT ASYMÉTRIQUE (PGP) : Système utilisant deux clés (une publique pour chiffrer, une privée pour déchiffrer).
- PROXY / VPN / TOR : Outils permettant de masquer l'adresse IP réelle en faisant transiter la connexion par des serveurs intermédiaires.

PARTIE 06 : PSYCHOLOGIE & ANALYSE CRIMINELLE

- MODUS OPERANDI (M.O.) : La méthode employée par le criminel pour commettre l'acte. Il peut évoluer avec l'expérience.
- SIGNATURE : Acte inutile pour le crime mais nécessaire à l'équilibre psychologique de l'auteur (ex: mise en scène du corps). Elle ne change jamais.
- PROFILAGE (Analyse Comportementale) : Déduction des caractéristiques probables de l'auteur à partir des traces laissées sur la scène.
- VICTIMOLOGIE : Étude de la victime pour comprendre pourquoi elle a été choisie (risque élevé, opportunité, lien caché).
- CERCLE DE CANTER : Théorie supposant que la majorité des criminels opèrent dans un rayon géographique proche de leur domicile ou d'un point d'intérêt.

"La tech évolue, les criminels aussi. Ce lexique n'est pas figé dans le marbre : je l'actualise au rythme de mes découvertes et des nouvelles procédures PTS. Reviens checker la version régulièrement pour ne pas rester sur une ancienne version de la vérité."