

La Bibliothèque de menaces est une base de connaissances de techniques répressives, de mesures d'atténuation qui peuvent être prises pour les contrer, et d'opérations répressives où elles ont été utilisées. Le but est d'aider les anarchistes et autres rebelles à comprendre les options à la disposition de leurs adversaires, développer des modèles de menaces adaptés, et au final réussir dans leurs actions et projets.



No Trace Project / Pas de trace, pas de procès. Un ensemble d'outils pour aider les anarchistes et autres rebelles à **comprendre** les capacités de leurs ennemis, **saper** les efforts de surveillance, et au final **agir** sans se faire attraper.

Selon votre contexte, la possession de certains documents peut être criminalisée ou attirer une attention indésirable. Faites attention aux brochures que vous imprimez et à l'endroit où vous les conservez.

Bibliothèque de menaces

Partie 2/5

Techniques S-Sc



4 novembre 2025

Un résumé des mises à jour depuis cette date est disponible sur :
notrace.how/threat-library/fr/changelog.html

Cette brochure est divisée en plusieurs parties. Les chapitres dans la partie actuelle sont référencés par leurs numéros de page. Les chapitres dans d'autres parties sont référencés par le symbole # suivi du numéro de la partie.

Bibliothèque de menaces

Partie 1/5 : À propos, Tactiques, Techniques A–P

Partie 2/5 : Techniques S–Sc

Partie 3/5 : Techniques Su–V

Partie 4/5 : Mesures d'atténuation

Partie 5/5 : Opérations répressives, Pays, Tutoriel, Contribuer

Texte d'origine en français

No Trace Project

notrace.how/threat-library/fr

qui montraient leurs visages découverts alors qu'ils étaient dans le métro, peu avant ou après l'action.⁴⁷

Répression de l'attaque sur le siège de Clarín (#5) : Les enquêteurs ont utilisé un logiciel de reconnaissance faciale pour identifier l'un·e des inculpé·e·s, à partir d'une photo de son visage extraite d'images de vidéosurveillance filmées près du lieu de l'attaque.³³

⁴⁷<https://notrace.how/documentation/monica-and-francisco-2013-case-file.pdf>

Sommaire

3. Techniques	3
3.18. Science forensique	3
3.18.1. ADN	3
3.18.2. Analyse de l'écriture	13
3.18.3. Autres traces physiques	17
3.18.4. Balistique	25
3.18.5. Empreintes digitales	26
3.18.6. Incendie volontaire	28
3.18.7. Linguistique	36
3.18.8. Numérique	38
3.18.9. Reconnaissance de démarche	41
3.18.10. Reconnaissance faciale	44

La reconnaissance faciale implique qu'un humain ou un système automatisé localise et mesure les caractéristiques (par exemple la forme du nez, la distance entre les yeux) d'un visage (ou d'une photo d'un visage), et les compare avec les caractéristiques d'un autre visage (ou photo d'un visage). Si les caractéristiques des deux visages sont suffisamment proches, on considère que les visages appartiennent à la même personne.

Les systèmes modernes de reconnaissance faciale sont capables de comparer la photo d'un visage à une vaste base de données de visages, même si le visage est masqué, avec seulement les yeux et sourcils visibles. Des systèmes de reconnaissance faciale associés à la **vidéosurveillance de masse (#3)** peuvent être utilisés pour automatiser le suivi d'individus à travers un espace.

Voir le sujet « Reconnaissance faciale ».⁴⁶

MESURES D'ATTÉNUATION

Dissimulation biométrique (#4) : Tu peux porter un masque qui cache les caractéristiques de ton visage, et des lunettes de soleil ou un chapeau à bord bas pour couvrir tes yeux.

Tenue anonyme (#4) : Tu peux porter un masque qui couvre correctement ton visage, y compris tes sourcils et jusqu'en haut de ton nez.

OPÉRATIONS RÉPRESSIVES

Opération de 2019-2020 contre Mónica et Francisco (#5) : Pour identifier Mónica et Francisco sur les images de vidéosurveillance publique, des photos des deux ont été comparées aux images, avec une comparaison de plusieurs caractéristiques du visage : distance entre les yeux, rides, cicatrices de piercing, taille des oreilles, formes de la bouche et du nez.⁷

Opération de 2013 contre Mónica et Francisco (#5) : La principale preuve contre Mónica et Francisco était une comparaison de photos des deux avec des images de vidéosurveillance publique

⁴⁶<https://notrace.how/resources/fr/#topic=facial-recognition>

3. Techniques

3.18. Science forensique

Utilisée par la tactique : **Incrimination**

La science forensique est l'application de la science aux enquêtes pour la collecte, la préservation, et l'analyse de preuves. Elle recouvre un ensemble de domaines : analyse ADN, analyse d'empreintes digitales, analyse de tâches de sang, balistique judiciaire, analyse de traces laissées par des outils, sérologie, toxicologie, analyse de cheveux et de fibres, analyse d'empreintes de pas et de traces de pneus, analyse chimique des drogues, analyse de la peinture et des débris de verre, linguistique, analyse numérique du son, de la vidéo et de l'image, etc.

En plus de relier l'identité d'un suspect à une action, la science forensique est souvent utilisée pour relier ensemble des actions distinctes.

Les experts en science forensique témoignent souvent en tant qu'experts judiciaires lors de procès.

3.18.1. ADN



Prélèvement d'un échantillon ADN à l'aide d'un écouvillon.

Préparation minutieuse de l'action (#4) : Un adversaire peut utiliser la reconnaissance de démarche pour analyser ta démarche sur des images de vidéosurveillance sur ou à proximité du lieu d'une action. Pour contrer ça, tu peux préparer minutieusement l'action pour éviter de te déplacer avec ta démarche normale près d'une caméra.

Tenue anonyme (#4) : Tu peux porter des vêtements amples pour cacher ta démarche.

OPÉRATIONS RÉPRESSIVES

Bialystok (#5) : La principale preuve contre la personne accusée d'une attaque explosive contre un commissariat était une comparaison de sa démarche et de la couleur de son manteau avec les caractéristiques correspondantes d'une personne filmée par les caméras de surveillance du commissariat.⁴⁴

Scintilla (#5) : Deux des personnes ont été accusées d'avoir commis un incendie volontaire parce que leurs démarches et la forme de leurs corps ont été considérés compatibles avec des personnes filmées par des caméras de vidéosurveillance en train de placer un bidon de liquide inflammable devant un bureau de poste italien.⁴⁵

Operation 8 (#5) : Une personne a été identifiée sur les vidéos des « camps d'entraînement » sur la base de sa taille, de sa démarche et de sa couleur de peau.¹¹

Répression de l'attaque sur le siège de Clarín (#5) : L'un·e des inculpé·e·s a été identifié·e parce que sa démarche correspondait à celle d'un·e suspect·e visible sur des images de vidéosurveillance filmées près du lieu de l'attaque.³³

3.18.10. Reconnaissance faciale

La reconnaissance faciale est l'analyse des caractéristiques des visages humains dans le but d'associer un visage à un autre.

⁴⁴<https://ilrovescio.info/2022/02/02/aggiornamento-sulle-misure-e-sul-processo-per-lop-byalistok>

⁴⁵<https://macerie.org/index.php/2019/04/17/ultime-da-carceri-e-tribunali>

- Est-ce que les deux personnes ont une démarche générique ou unique. Par exemple, une personne qui boîtit a une démarche assez unique.
- Est-ce que les deux personnes sont vues depuis le même angle réaliser le même type de mouvement (par exemple, soit marcher, soit courir).

Scénario typique

Voici un scénario typique dans lequel un adversaire utilise la reconnaissance de démarche :

- Une personne est filmée par une caméra de surveillance en train de mener une action. Elle n'est pas reconnaissable parce qu'elle porte une **tenue anonyme (#4)**. L'adversaire obtient la vidéo.
- Sur la base d'autres indices, l'adversaire suspecte quelqu'un d'avoir mené l'action. Il obtient une vidéo de cette suspect·e en train de se déplacer, via une caméra de surveillance près de son domicile, une caméra de surveillance lorsqu'il est en garde-à-vue, ou bien une **caméra cachée (#1)**.
- L'adversaire compare la démarche de la personne dans la première vidéo avec la démarche du/de la suspect·e dans la deuxième vidéo pour déterminer si ils pourraient ou non être la même personne, et la confiance dans cette détermination.

Voir aussi

Voir Forensic Gait Analysis: Principles and Practice²⁴ (*Analyse de démarche par la science forensique : principes et pratique*) pour une vue d'ensemble complète de l'analyse de démarche.

MESURES D'ATTÉNUATION

Dissimulation biométrique (#4) : Tu peux porter des vêtements amples qui cachent la forme de ton corps, utiliser un parapluie ou d'autres objets couvrants, ou changer drastiquement ton style de marche en adoptant une « démarche bizarre ».

La science forensique appliquée à l'ADN est la collecte et l'analyse d'échantillons ADN dans le but de faire correspondre des échantillons ADN à des individus.

L'ADN est la molécule qui contient le code génétique des organismes. Chaque cellule¹ dans un corps humain contient de l'ADN. L'ADN de chaque individu est unique, à l'exception des vrais jumeaux. Un adversaire peut comparer l'ADN d'un individu avec un échantillon ADN prélevé sur un objet ou un lieu et, s'ils correspondent, conclure que l'individu a probablement été en contact avec cet objet ou ce lieu.

Transfert

Les cellules du corps humain et l'ADN qu'elles contiennent peuvent être directement transférées du corps à l'environnement. Par exemple :

- Quand tu sues, urines, défèques, ou saignes, tu laisses de la sueur, de l'urine, des excréments, ou du sang.
- Quand tu respires ou parles, tu émettes des gouttelettes respiratoires depuis ta bouche et ton nez qui contiennent de la salive et du mucus.
- Quand tu touches une surface avec ta peau, des cellules de peau sont transférées de ta peau à la surface.
- Même quand tu ne fais rien, tu perds constamment des cellules de peau et des poils.

Les cellules du corps humain peuvent aussi être transférées indirectement. Par exemple, si tu touches l'extérieur d'une paire de gants avec tes doigts, puis que tu mets les gants et touches une poignée de porte, tes cellules de peau peuvent être transférées d'abord de tes doigts à l'extérieur des gants, puis de l'extérieur des gants à la poignée de porte.

Voir la section « Transfer » (*Transfert*) de la No Trace Project DNA Literature Review² (*Revue de la littérature sur l'ADN par*

¹À l'exception des globules rouges.

²<https://notrace.how/resources/fr/#dna-review>

le *No Trace Project*) pour plus de détails sur le transfert direct et indirect d'ADN.

Dégradation

L'ADN est très robuste et ne se dégrade pas facilement, mais peut se dégrader sous certaines conditions, par exemple en étant exposé à des températures élevées ou de l'hypochlorite de soude.

Voir la section « Dégradation » (*Dégradation*) de la *No Trace Project DNA Literature Review*² sur les conditions sous lesquelles l'ADN peut se dégrader.

Collecte

Un adversaire peut prélever un échantillon ADN :

- Sur une surface qui contient visiblement de l'ADN, comme une trace biologique visible (par exemple de la salive ou du sang).
- Sur une surface suspectée de contenir de l'ADN, comme une poignée de porte suspectée d'avoir été touchée par un·e suspect·e sur le lieu d'une action.

Un adversaire peut utiliser des techniques pour faciliter la collecte d'ADN, comme :

- Des techniques d'enlèvement de suie pour prélever des échantillons ADN cachés sous la suie après un feu.
- Du luminol pour localiser des échantillons de sang invisibles à l'oeil nu.

Analyse

Un adversaire peut analyser un échantillon ADN pour identifier des marqueurs génétiques de l'ADN. Une telle analyse fonctionne si :

- L'échantillon contient assez d'ADN. Par exemple, une goutte de sang contient significativement plus d'ADN que des

- Des facteurs intrinsèques : comment tu as appris à marcher, ton anatomie et ta physiologie, et tes éventuelles blessures ou pathologies.
- Des facteurs extrinsèques : tes vêtements et le terrain sur lequel tu te déplaces (plat ou non, avec ou sans obstacles...)

Analyse

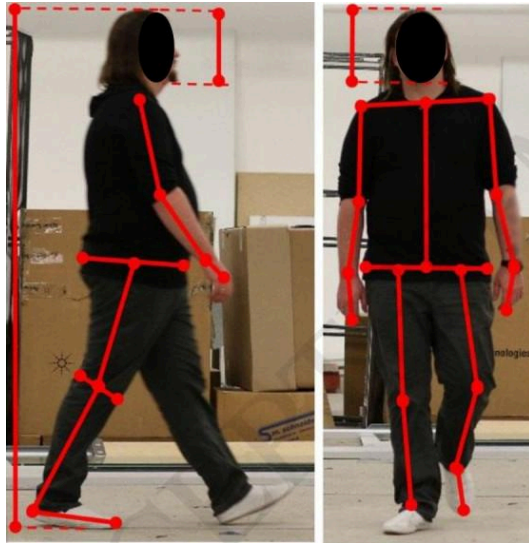
Un adversaire qui te regarde te déplacer peut localiser, mesurer, et catégoriser tes caractéristiques corporelles (position de tes chevilles, genoux, hanches...) à différentes étapes du mouvement et les comparer aux caractéristiques corporelles d'une autre personne qui se déplace. Cette comparaison peut permettre à l'adversaire de déterminer si tu pourrais ou non être cette autre personne, mais ne permet généralement pas à l'adversaire de déterminer avec certitude que tu es cette autre personne. Cette comparaison est généralement faite par des humains, parfois assistés de logiciels spécialisés.

La reconnaissance de démarche se fait typiquement en comparant deux ensembles d'images de vidéosurveillance. Le premier ensemble montre une première personne qui se déplace, et le deuxième ensemble une deuxième personne qui se déplace. Le but de la comparaison est de déterminer si la première personne pourrait ou non être la deuxième personne. La solidité de la comparaison, c'est-à-dire, la confiance dans la détermination que la première personne pourrait ou non être la deuxième personne, dépend de plusieurs facteurs, y compris :

- La qualité et le nombre d'images par seconde des images de vidéosurveillance.
- L'éclairage de la scène.
- Est-ce que les deux personnes sont suffisamment proches de la caméra, sont entièrement visibles, font plusieurs pas, et portent des vêtements qui ne cachent pas excessivement leur démarche.

- « Hibou », un nom utilisé par des personnes en lutte contre Cigéo pour s'auto-désigner.
- « Incendie ».

3.18.9. Reconnaissance de démarche



Gauche : une personne marche, vue de côté. Droite : la même personne marche, vue de devant. Des lignes rouges marquent certaines des caractéristiques corporelles utilisées pour la reconnaissance de démarche.

La reconnaissance de démarche (aussi connue sous le nom d'*analyse de démarche*) est l'analyse de la manière et du style de déplacement des individus dans le but d'associer une manière ou style à un autre.

Facteurs de la démarche

Quand tu te déplaces, tu adoptes naturellement une démarche relativement unique qui dépend de plusieurs facteurs, y compris :

cellules de peau laissées par un bref contact entre la peau et une surface.

- L'ADN n'est pas trop dégradé.
- Tout ou la majorité de l'ADN dans l'échantillon provient d'au plus trois individus.

Un adversaire peut comparer *deux* échantillons ADN analysés avec succès pour :

- Déterminer s'ils proviennent du même individu. Par exemple, il peut comparer un échantillon ADN prélevé de la bouche d'un suspect en garde-à-vue à un échantillon ADN prélevé sur le lieu d'une action et, s'ils correspondent, conclure que le/la suspect(e) était probablement présent(e) sur le lieu de l'action.
- Déterminer s'ils proviennent d'individus proches génétiquement, comme des parents et leurs enfants, des frères et sœurs, ou des cousins.

Un adversaire peut aussi utiliser *un seul* échantillon ADN analysé avec succès pour :

- Déterminer le sexe génétique de l'individu.
- Tenter de prédire l'apparence de l'individu grâce au phénotypage de l'ADN. Actuellement les couleurs des yeux, des cheveux et de la peau peuvent être prédites avec un haut degré de précision, et des recherches sont en cours pour tenter de prédire d'autres caractéristiques. Cette technique n'est pas utilisée dans tous les contextes.

Bases de données ADN

Dans de nombreux pays, l'État a des bases de données ADN contenant l'ADN de nombreux individus, souvent obtenu lors d'arrestations ou dans le cadre de condamnations.

Des pays peuvent s'échanger des données ADN via :

- Des bases de données ADN internationales, comme la base de données ADN d'Interpol ou le système d'information Europol.

- Des bases de données ADN nationales reliées ou mises en réseau. Par exemple, les États membres de l'Union Européenne sont tenus de maintenir une base de données ADN à laquelle les autres États membres peuvent accéder.
- L'échange de données ADN à la demande, typiquement dans des cas de crimes graves.

Voir aussi

- « blablaADN. Tout cramer pour brûler + longtemps : un guide pour ne pas laisser de traces »³ pour une vue d'ensemble de la science forensique appliquée à l'ADN.
- La No Trace Project DNA Literature Review² pour un ensemble de détails utiles sur la science forensique appliquée à l'ADN, issus de la littérature universitaire.
- Le sujet « ADN ».⁴

MESURES D'ATTÉNUATION

Gants (#4) : Tu peux porter des gants pour éviter de laisser de l'ADN sur les surfaces que tu touches.

Protocoles de minimisation de l'ADN (#4) : Tu peux minimiser la quantité d'ADN que tu laisses sur une surface pour minimiser le risque qu'un adversaire puisse utiliser la science forensique appliquée à l'ADN pour aboutir à une conclusion utile à partir d'une analyse de la surface.

Préparation minutieuse de l'action (#4) : Un adversaire peut utiliser la science forensique appliquée à l'ADN pour prélever de l'ADN sur le lieu d'une action. Pour contrer ça, tu peux préparer minutieusement l'action pour minimiser les traces ADN sur le lieu de l'action. Par exemple, tu peux :

- Ranger tes cheveux sous un couvre-chef.
- Si tu dois découper une clôture, faire des trous suffisamment grands pour pouvoir passer à travers sans toucher la clôture.

³<https://notrace.how/resources/fr/#blabladn>

⁴<https://notrace.how/resources/fr/#topic=dna>

Effacement et protection des métadonnées (#4) : Un adversaire peut utiliser la science forensique appliquée au numérique pour extraire et analyser des métadonnées. Pour contrer ça, tu peux effacer les métadonnées de fichiers avant de les publier en ligne ou de les envoyer à des gens.

Éviter l'auto-incrimination (#4) : Un adversaire peut utiliser la science forensique appliquée au numérique pour extraire des informations auto-incriminantes d'un appareil numérique. Pour contrer ça, tu peux éviter de stocker de telles informations sur des appareils numériques à part pour des raisons mûrement réfléchies (par exemple écrire et envoyer un communiqué de revendication tout en adoptant de **bonnes pratiques numériques (#4)**).

OPÉRATIONS RÉPRESSIVES

Opération contre Revolutionära fronten (#5) : Les enquêteurs ont analysé l'ordinateur de l'un·e des inculpé·e·s, saisi lors d'une perquisition, et ont récupéré les messages envoyés et reçus par l'inculpé·e sur l'application de messagerie MSN Messenger.¹¹ Les messages comprenaient :

- Une discussion détaillée du tabassage de Stockholm, y compris la mention des noms de certain·e·s des inculpé·e·s comme ayant participé au tabassage.
- Une discussion de la visite nocturne au domicile du fasciste, y compris la mention des noms des habitants de la maison et la mention des noms de certain·e·s des inculpé·e·s comme ayant participé à la visite.

Affaire de l'association de malfaiteurs de Bure (#5) : Les enquêteurs ont analysé des supports de stockage en extrayant automatiquement les fichiers contenant les mots clés suivants en rapport avec l'enquête :¹¹

- « Action ».
- « Andra », l'agence en charge du projet Cigéo.
- « Bindeuil », le nom du bâtiment attaqué pendant la manifestation du 21 juin 2017.

La science forensique appliquée au numérique est l'extraction, le stockage, et l'analyse des données numériques qui peuvent être utiles dans le cadre d'enquêtes. Cela inclut les données provenant d'ordinateurs, de téléphones, de disques dur, et autres supports de stockage.

Par exemple, cette discipline peut être utilisée pour récupérer un fichier « supprimé » du disque dur d'un ordinateur, récupérer l'historique de navigation web d'un téléphone, ou déterminer comment un serveur a été piraté.

MESURES D'ATTÉNUATION

Bonnes pratiques numériques (#4) : Un adversaire peut utiliser la science forensique appliquée au numérique pour extraire des données d'un appareil numérique que tu as utilisé. Pour contrer ça, tu peux adopter de bonnes pratiques numériques et, en particulier, utiliser Tails,⁴³ un système d'exploitation « amnésique » conçu pour ne pas laisser de traces sur l'ordinateur sur lequel il est utilisé.

Lorsqu'il enquête sur une cyber-action, un adversaire peut utiliser la science forensique appliquée au numérique pour analyser les cibles de l'action et déterminer d'où provient l'action, un processus appelé *attribution* qui peut impliquer de déterminer quels outils ont été utilisés pour l'action et toute autre « signature » numérique. Quand tu effectues une cyber-action, tu peux adopter de bonnes pratiques numériques pour que ce soit plus difficile pour un adversaire de réussir cette attribution. Par exemple, tu peux :

- Utiliser des outils populaires plutôt que sur mesure.
- Si tu utilises un Virtual Private Server (VPS), **achète-le anonymement (#4)** et accède-y avec Tails.⁴³

Chiffrement (#4) : Un adversaire peut utiliser la science forensique appliquée au numérique pour extraire des données d'appareils numériques non chiffrés. Pour contrer ça, tu peux chiffrer tes appareils numériques avec le chiffrement complet du disque et un mot de passe robuste.

⁴³<https://tails.net/index.fr.html>

- T'assurer que les surfaces sur le lieu de l'action ne soient pas touchées si ce n'est pas nécessaire, et que les surfaces avec lesquelles il faut interagir (comme une poignée de porte) soient touchées par une personne qui met en place des **protocoles de minimisation de l'ADN (#4)**.
- T'assurer que rien n'est laissé sur place accidentellement comme un sac, un outil, ou quelque chose qui pourrait tomber d'une poche.

OPÉRATIONS RÉPRESSIVES

Scripta Manent (#5) : Des preuves ADN ont été utilisées pour condamner Alfredo Cospito.⁵

Opération contre Boris (#5) : La seule preuve contre Boris était que son ADN a été trouvé sur un bouchon de bouteille au pied d'une des antennes brûlées dans le sabotage d'avril.⁶

Lorsque l'ADN d'une personne proche de Boris a été prélevé pendant une perquisition, seulement huit heures et demi se sont écoulées entre le prélèvement de l'échantillon ADN et le résultat de sa comparaison avec d'autres traces prélevées antérieurement.

Opération de 2019-2020 contre Mónica et Francisco (#5) : L'ADN de Francisco a été trouvé sur le colis piégé envoyé à l'ancien ministre de l'Intérieur, qui a été désamorcé et n'a pas explosé.⁷

Répression contre Zündlumpen (#5) : Dans certaines des perquisitions, des échantillons ADN ont été prélevés sur un mégot de cigarette,⁸ des brochures,⁹ des livres, des portes, des tasses, et des machines d'impression.

⁵<https://insuscettibilediravvedimento.noblogs.org/post/2020/03/29/it-en-italia-su-una-sentenza-e-qualcosa-daltro-un-testo-di-marco-dal-carcere-di-alessandria>

⁶<https://rupture.noblogs.org/post/2023/10/04/no-bars>

⁷<https://notrace.how/resources/fr/#monica-francisco>

⁸<https://notrace.how/resources/fr/#chretien-de-baviere>

⁹<https://notrace.how/resources/fr/#gendarmes-et-voleurs>

Renata (#5) : Après son arrestation et emprisonnement, la personne accusée de l'attaque explosive contre le siège social de Lega Nord à Trévise a refusé que son ADN soit prélevé.¹⁰ Peu de temps après le refus de la personne, des matons ont cherché sa cellule et secrètement remplacé un peigne par un autre, vraisemblablement pour obtenir l'ADN de la personne à partir des cheveux sur le peigne qu'ils ont pris.

Recherche d'un·e fugitive (#5) : Suite à l'attaque du bâtiment en 2020, des échantillons ADN ont été prélevés sur des morceaux de verre brisé, des stores, le trottoir à l'extérieur du bâtiment, ainsi que sur du sang retrouvé sur une bouteille d'essence à briquet et d'autres objets.¹¹ Il semble qu'à ce stade, les échantillons ne correspondaient à personne dans les bases de données ADN.

En 2023, la personne a été condamnée dans une autre affaire dans un État autre que la Géorgie. Dans le cadre de cette condamnation, elle a été contrainte de fournir un échantillon ADN à la police, qui a correspondu aux échantillons prélevés en 2020.

Répression du sabotage de l'usine Lafarge (#5) : Dans l'une des premières perquisitions, la police a insisté pour que les personnes arrêtées portent des masques chirurgicaux pour se protéger du Covid : les masques ont ensuite été saisis pour y prélever de l'ADN.¹² Une personne qui avait refusé de porter un masque s'est faite confisquer des sous-vêtements en garde-à-vue, vraisemblablement pour y prélever son ADN.¹³

Prometeo (#5) : Des traces ADN ont été utilisées pour condamner la personne accusée d'avoir brûlé un DAB.¹⁴

Mauvaises intentions (#5) : Lors des gardes-à-vue, de l'ADN a été prélevé sur les vêtements des personnes et sur des gobelets en

¹⁰<https://web.archive.org/web/20210518112509/https://roundrobin.info/2020/03/aggiornamenti-su-manu-stecco-juan-e-sasha>

¹¹Source non publique.

¹²<https://sansnom.noblogs.org/archives/16831>

¹³<https://notrace.how/resources/fr/#lafarge>

¹⁴<https://web.archive.org/web/20210612231740/https://roundrobin.info/2021/05/sentenza-beppe>

OPÉRATIONS RÉPRESSIVES

Scripta Manent (#5) : Des textes publiés par certain·es des accusé·es ont été comparés aux communiqués de revendication de la Fédération Anarchiste Informelle, dans le but de prouver que les accusé·es avaient écrit ces communiqués.²⁵

Répression contre Zündlumpen (#5) : Les enquêteurs ont comparé des textes du journal Zündlumpen à des lettres privées trouvées dans des perquisitions, dans l'espoir de prouver que des personnes avaient écrit dans le journal.⁹

Opération contre Direct Action (#5) : Les enquêteurs ont remarqué des similitudes linguistiques entre des communiqués de revendication publiés par Direct Action et des articles d'une publication trimestrielle locale nommée *Resistance*.⁴² Cela les a mené à identifier une contributrice à *Resistance*, qui était une amie de membres de Direct Action, et à la placer sous **surveillance physique (#3)**.

3.18.8. Numérique



Un Cellebrite Universal Forensics Extraction Device (UFED) qui extrait les données d'un iPhone 4S, 2013.

⁴²<https://archive.org/details/direct-action-memoirsofan-urban-guerrilla>

Identification de l'auteur

L'identification de l'auteur peut être utilisée pour déterminer, par exemple :

- Qui a écrit un communiqué de revendication anonyme publié sur Internet ou envoyé à un journal.
- Si plusieurs communiqués de revendication anonymes ont été écrits par la même personne ou le même groupe.
- Qui a rédigé un plan relatif à des activités illégales trouvé pendant une **perquisition (#1)**, une **visite discrète de domicile (#3)** ou une arrestation.

Identification de la voix

L'identification de la voix peut être utilisée pour déterminer, par exemple :

- Qui parle sur une conversation téléphonique interceptée ou un enregistrement fait par un **microphone caché (#1)**.
- Qui a appelé les autorités pour faire une alerte à la bombe.

Voir aussi

À propos d'identification de l'auteur :

- Counteracting Forensic Linguistics⁴⁰ (*Contrer la science forensique appliquée à la linguistique*).
- Qui a écrit ça ?⁴¹

MESURES D'ATTÉNUATION

Dissimulation biométrique (#4) : Tu peux cacher les propriétés acoustiques de ta voix pour contrer l'identification de la voix.

Masquer son style d'écriture (#4) : Tu peux cacher ton style d'écriture pour contrer l'identification de l'auteur.

⁴⁰<https://anonymousplanet.org/guide/appendix-a4-counteracting-forensic-linguistics>

⁴¹<https://notrace.how/resources/fr/#qui-a-ecrit>

plastique.¹⁵ Dans un cas, seulement neuf heures se sont écoulées entre le prélèvement d'un échantillon ADN en garde-à-vue et le résultat de sa comparaison à un autre échantillon prélevé antérieurement.

Les accusations contre une personne étaient basées sur une correspondance entre son ADN et l'ADN prélevé sur le lieu de la tentative d'incendie contre l'armoire électrique. Des échantillons ADN ont été prélevés sur un gant en latex trouvé à proximité et sur une bouteille à l'intérieur de l'armoire—qui n'a pas brûlé à cause d'un retardateur défectueux.

Les accusations contre d'autres personnes étaient basées sur une correspondance entre leur ADN et l'ADN prélevé sur une cigarette utilisée comme retardateur pour un dispositif incendiaire—le retardateur n'a pas fonctionné et a été retrouvé intact sous la dépanneuse de la police.

Opération contre Amos Mbedzi (#5) : L'ADN de Mbedzi a été retrouvé sur un coussin et un pare-soleil de la voiture utilisée pour transporter l'engin explosif jusqu'au lieu de l'explosion.¹⁶

Opération contre Louna (#5) : Des échantillons ADN correspondant à l'ADN de Louna ont été prélevés sur :¹¹

- Un sac poubelle et un masque chirurgical partiellement brûlés, saisis près de la pelleteuse incendiée.
- Un short, saisi dans sa chambre d'hôpital pendant son hospitalisation.
- Un gobelet en carton saisi lors de son entrée en garde-à-vue.
- Une cuillère et une serviette saisies pendant sa garde-à-vue, après un repas.

Des échantillons ADN correspondant à l'ADN d'une personne ayant été vue dans les couloirs de l'hôpital demandant des nouvelles de Louna ont été prélevés sur :

¹⁵<https://infokiosques.net/spip.php?article597>

¹⁶<https://notrace.how/documentation/case-against-amos-mbedzi-case-file.pdf>

- Un short, saisi dans la chambre d'hôpital de Louna pendant son hospitalisation.
- Un masque chirurgical retrouvé dans le short.

Des échantillons ADN non exploitables ont été prélevés sur :

- Un marteau partiellement brûlé retrouvé dans la cabine de la pelleuse incendiée, dont la fenêtre avait été brisée.
- Une torche—un bout de bois avec à son extrémité un tissu imbibé de liquide inflammable—retrouvée près de la pelleuse incendiée.

Répression du premier incendie de Jane's Revenge (#5) : En mai 2022, des échantillons ADN ont été prélevés sur plusieurs objets trouvés par les enquêteurs sur le lieu de l'action, dont une fenêtre cassée, un pot en verre, un briquet, et un cocktail Molotov intact.¹⁷ En mars 2023, la police a vu la personne jeter un sac contenant un burrito en partie mangé dans une poubelle publique. Des échantillons ADN prélevés sur le contenu du sac correspondaient aux échantillons prélevés sur le lieu de l'action.

Scintilla (#5) : L'accusation contre Peppe était basée sur une correspondance entre des traces ADN trouvées à l'intérieur du colis piégé et son ADN prélevé sur un mégot de cigarette au cours de l'enquête.¹⁸

Affaire de l'association de malfaiteurs de Bure (#5) : Des échantillons ADN ont été prélevés sur :¹¹

- Des objets récupérés après des manifestations, dont des feux d'artifice, des cocktails Molotov, un briquet, et des cailloux utilisés pour briser des fenêtres.
- Des objets trouvés dans des perquisitions, dont des vêtements, des masques à gaz, des casques, et des récipients contenant de l'essence ou autres substances.

¹⁷<https://notrace.how/documentation/first-jane-s-revenge-arson-investigation-files.pdf>

¹⁸<https://web.archive.org/web/20200918130026/https://roundrobin.info/2019/12/verona-una-perquisizione-e-un-arresto>

OPÉRATIONS RÉPRESSIVES

Mauvaises intentions (#5) : Des échantillons ADN ont été prélevés sur une cigarette utilisée comme retardateur pour un dispositif incendiaire—le retardateur n'a pas fonctionné et a été retrouvé intact sous la dépanneuse de la police.¹⁵

Opération contre Louna (#5) : Un détecteur de gaz³⁹ a été utilisé, sans succès, pour détecter des traces d'accélérateurs dans la cabine de la pelleuse incendiée.¹¹

Des traces d'accélérateurs ont été prélevées :

- Sur une torche—un bout de bois avec à son extrémité un tissu imbibé de liquide inflammable—retrouvée près de la pelleuse incendiée.
- À l'intérieur de la pelleuse incendiée.

Des traces d'accélérateurs ont été recherchées, sans succès, sur les vêtements de Louna, saisis à l'hôpital pendant son hospitalisation.

Répression du premier incendie de Jane's Revenge (#5) : Des échantillons ADN ont été prélevés sur un cocktail Molotov intact trouvé par les enquêteurs sur le lieu de l'action.¹⁷

Affaire de l'association de malfaiteurs de Bure (#5) : Des traces d'accélérateurs ont été collectées sur des objets récupérés après des manifestations, et analysées.¹¹

3.18.7. Linguistique

La science forensique appliquée à la linguistique est l'application de connaissances linguistiques pour identifier l'auteur d'un texte ou la personne derrière une voix. L'identification de l'auteur (aussi appelée *stylométrie*) est basée sur l'analyse de certains schémas d'utilisation du langage : vocabulaire, collocations, orthographe, grammaire, etc. L'identification de la voix est basée sur les unités phonétiques et les caractéristiques acoustiques de la voix.

³⁹https://en.wikipedia.org/wiki/Gas_detector

- Construire les dispositifs de test avec des composants de même marque et de même modèle que les composants que tu utiliseras pour le vrai dispositif.
- Stocker les dispositifs de test dans les mêmes conditions (par exemple d'humidité) que le vrai dispositif, et pour la même durée.
- Transporter les dispositifs de test de la même manière que le vrai dispositif.
- Installer les dispositifs de test dans les mêmes conditions que le vrai dispositif (conditions météorologiques, température, obscurité, etc.)
- T'assurer que tu seras capable de construire, transporter, et installer le dispositif dans les conditions psychologiques de l'action (stress).

Si tu utilises un accélération dans une action et qu'un adversaire prend la peine de collecter des échantillons d'accélération à des fins de comparaison (par exemple, des échantillons d'essence provenant de stations-service), il pourrait identifier la source de l'accélération que tu as utilisé. Pour contrer ça, tu peux :

- Réduire le risque d'identification en utilisant un mélange d'accélération du même type provenant de différentes sources (par exemple, de l'essence provenant de différentes stations-service).
- Réduire encore davantage le risque d'identification en utilisant un mélange d'accélération du même type provenant de sources situées dans des secteurs différents (afin que la composition chimique des accélération soit plus distincte) et en laissant passer du temps entre le moment où tu te procures les accélération et le moment où tu les utilises (afin que l'adversaire ne puisse pas obtenir rétroactivement les échantillons dont il aurait besoin pour la comparaison, car les réservoirs des stations-service où tu t'es procuré les accélération auront été remplis).

Les enquêteurs n'ont pas réussi à faire correspondre à qui que ce soit la grande majorité des échantillons ADN qu'ils ont prélevés. Les exceptions notables étaient :

- Un échantillon ADN prélevé sur un cocktail Molotov trouvé dans une perquisition a correspondu à une personne dans le Fichier national automatisé des empreintes génétiques (FNAEG).
- Un échantillon ADN prélevé sur le bouchon d'un bocal contenant des matières pouvant servir à construire des engins explosifs, trouvé dans une perquisition, a correspondu à une personne dans le FNAEG.
- Un échantillon ADN prélevé sur un briquet retrouvé après une manifestation a correspondu à une autre trace d'une affaire plus ancienne sans lien avec l'affaire en cours, mais n'a correspondu à personne dans le FNAEG.

Opération contre Ruslan Siddiqi (#5) : Des échantillons ADN ont été prélevés sur des personnes vivant dans une vaste zone autour du site de l'attaque à l'explosif contre le train, y compris sur des soldats et des citoyens ukrainiens, probablement parce qu'ils étaient considérés comme de potentiels suspects.¹⁹

Opération à Nea Filadelphia (#5) : Les accusations contre plusieurs personnes étaient basées sur une correspondance entre leur ADN, prélevé de force en garde-à-vue, et des échantillons ADN prélevés sur des « objets mobiles » près des lieux des braquages.²⁰

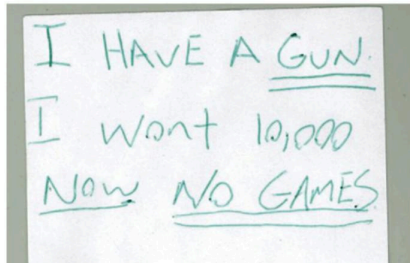
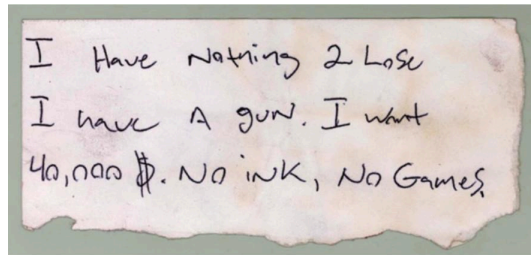
Panico (#5) : Des traces ADN étaient la seule preuve contre l'un des accusés.²¹

¹⁹<https://theins.ru/en/society/280988>

²⁰<https://abcsolidaritycell.espivblogs.net/archives/130>

²¹<https://panicoanarchico.noblogs.org>

3.18.2. Analyse de l'écriture



Deux notes utilisées lors de braquages²² montrant des similarités dans la formation du nombre « 0 ».

L'analyse de l'écriture (aussi connue sous le nom de *reconnaissance de l'écriture*) est l'analyse d'échantillons écrits, typiquement dans le but d'associer un échantillon à un autre.

Facteurs de l'écriture

Quand tu écris, tu adoptes naturellement une écriture relativement unique qui dépend de plusieurs facteurs, dont :

- Comment tu as appris à écrire : comment tu as appris à former les lettres et à déplacer l'instrument d'écriture.
- Tes habitudes d'écriture : ta façon personnelle de former les lettres et de déplacer l'instrument d'écriture, qui peut être plus ou moins proche de comment tu as appris.
- Ton niveau d'écriture : est-ce que tu apprends à écrire ou est-ce que tu es expérimenté.e.

²²Certains braquages de banques sont effectués en passant discrètement une note écrite au guichet afin d'attirer aussi peu l'attention que possible.

de flammes éphémère sans plus de dégâts. An adversaire pourrait analyser avec succès l'ADN dans la trace de salive.

- Des cellules de peau ont été laissées à l'extérieur d'un dispositif incendiaire. Le dispositif a été activé et les objets autour ont pris feu, donnant lieu à un feu soutenu qui a enveloppé le dispositif pendant plusieurs minutes. Un adversaire ne devrait pas pouvoir analyser avec succès l'ADN dans les cellules de peau.

Voir « Incendiary Devices: Investigation and Analysis »²⁴ (*Dispositifs incendiaires : enquête et analyse*), chapitre « The Analysis of Incendiary Devices » (*L'analyse de dispositifs incendiaires*) pour une vue d'ensemble détaillée des enquêtes sur des dispositifs incendiaires.

MESURES D'ATTÉNUATION

Achats anonymes (#4) : Un adversaire peut relier les accéléranants et les composants de dispositifs incendiaires à l'endroit où ils ont été achetés, puis à l'identité de la personne qui les a achetés. Pour contrer ça, tu peux acheter les accéléranants³⁸ et les composants de dispositifs anonymement.

Préparation minutieuse de l'action (#4) : Si tu utilises un dispositif incendiaire dans une action et que celui-ci échoue, un adversaire peut récupérer le dispositif intact ou partiellement intact et potentiellement trouver beaucoup plus de preuves que si le dispositif n'avait pas échoué. Pour contrer ça, tu peux :

- Fabriquer et utiliser plusieurs dispositifs de test semblables au « vrai » dispositif que tu utiliseras dans l'action. Tu devrais mener les tests avec de bonnes précautions de sécurité puisque mener de tels tests peut être incriminant. Tu peux notamment :

³⁸Si c'est trop difficile d'acheter des accéléranants anonymement dans ton contexte (par exemple parce que c'est trop suspect d'acheter de l'essence à une station-service sans arriver en voiture), tu peux préférer les acheter de manière non anonyme et contrer cette technique par d'autres moyens.

telle manipulation peut être causée par le stress, l'obscurité ou l'inexpérience.

- Les conditions météorologiques pendant le stockage du dispositif (entre sa fabrication et son utilisation), en particulier s'il comporte des composants sensibles à l'humidité.
- Les conditions météorologiques sur les lieux de l'incendie : vent, rosée, brouillard et pluie.

Lorsqu'il analyse un dispositif incendiaire ou ses restes brûlés ou partiellement brûlés, un adversaire peut analyser :

- Les accélérateurs contenus dans le dispositif, ou les ILRs laissés sur le dispositif.
- Les **traces ADN** (p. 3) et **empreintes digitales** (p. 26) laissées lors de la manipulation des composants du dispositif.
- Les **marques d'outil** (p. 17) laissées lors de la construction du dispositif.
- Les identifiants visibles sur les composants de l'appareil, comme des numéros de série ou des codes-barres.
- Les **traces de verre** (p. 17), si le dispositif comporte des composants en verre.
- Les détails de la construction du dispositif, y compris l'utilisation de scotch et de colle, ainsi que la manière dont les composants sont branchés, soudés ou noués ensemble.

Un adversaire peut analyser avec succès une trace ADN laissée sur un dispositif incendiaire même si le dispositif a pris feu, selon le type de trace, la température à laquelle elle a été exposée, et la durée de l'exposition.³⁷ Par exemple :

- Une trace de salive a été laissée à l'extérieur d'un cocktail Molotov fait à partir d'une bouteille en verre. Le cocktail Molotov a été jeté et s'est cassé mais a juste produit une boule

- Ton instrument d'écriture : stylo, crayon, pinceau, bombe de peinture, etc.
- Où est-ce que tu tiens l'instrument d'écriture : dans ta main droite, ta main gauche, un pied, ta bouche, une prothèse, etc.
- Comment est-ce que tu tiens l'instrument d'écriture : par exemple, sur quels doigts repose un stylo quand tu écris.
- La surface d'écriture : papier, tissu, béton, etc.
- Ta posture quand tu écris : assis·e, debout, etc.
- Ton environnement d'écriture : par exemple, si tu écris avec des gants ou dans un véhicule en mouvement.
- Ton état physique et mental quand tu écris : fatigue, stress, état altéré par l'alcool, des drogues ou des médicaments, etc.

Analyse

Un adversaire peut analyser un échantillon écrit pour identifier ses caractéristiques, dont :

- La mise en page du texte : marges, espace entre les lignes, et parallélisme des lignes. Dans le cas des enveloppes : le style, la taille, et la position de l'adresse sur l'enveloppe.
- Le style d'écriture : par exemple écriture cursive ou scripte.
- L'espace entre les caractères et entre les mots.
- Les liens ou séparations entre les caractères.
- Le design et la construction des caractères : la forme des caractères, est-ce qu'un caractère est représenté par une ou plusieurs formes à travers l'échantillon, l'ordre dans lequel une forme est tracée, est-ce que et comment une forme est affectée par les formes particulières qui la précèdent et la suivent, et la taille des formes.
- Les traits tracés lorsque l'instrument d'écriture atteint et quitte la surface d'écriture, y compris leur taille, direction, chemin, et soudaineté.
- La pression exercée par l'instrument d'écriture sur la surface d'écriture.

³⁷Pour plus d'informations voir la section « Dégradation » (*Dégradation*) de la No Trace Project DNA Literature Review^a (*Revue de la littérature sur l'ADN par le No Trace Project*).

^a<https://notrace.how/resources/fr/#dna-review>

- La position de l'instrument d'écriture par rapport à la surface d'écriture.

Dans certaines langues écrites horizontalement, comme le français, un adversaire peut aussi identifier les caractéristiques suivantes :

- Est-ce que la ligne de base²³ est droite ou varie à travers l'échantillon.
- L'inclinaison de l'écriture : l'inclinaison prédominante des caractères par rapport à la ligne de base.

Un adversaire peut comparer les caractéristiques d'un échantillon d'écriture aux caractéristiques d'un autre pour déterminer si les échantillons ont été écrits ou non par la même personne, et la confiance dans cette détermination. Cette comparaison peut être faite par des humains ou par des logiciels spécialisés.

Bases de données d'échantillons

Dans certains pays, l'État a des bases de données d'échantillons d'écriture qui permettent de comparer un échantillon à tous les échantillons de la base de données. Par exemple, aux États-Unis, le Federal Bureau of Investigation (FBI) gère le Bank Robbery Note File (BRNF, *Fichier des notes de braquages*), qui contient des échantillons d'écriture utilisés lors de braquages de banque.

Voir aussi

Voir aussi Huber and Headrick's Handwriting Identification: Facts and Fundamentals²⁴ (*L'identification de l'écriture par Huber et Headrick : faits et fondamentaux*) pour une vue d'ensemble complète de l'analyse d'écriture.

²³ La ligne de base est la ligne horizontale sur laquelle les caractères reposent. Par exemple, la « boucle » d'un « p » minuscule repose sur la ligne de base, tandis que sa « queue » s'étend sous la ligne de base.

²⁴ Disponible sur la Surveillance Archive.^a

^a<https://notrace.how/fr/surveillance-archive.html>

identifier la marque de l'essence (si des échantillons sont prélevés dans les raffineries chaque fois qu'un lot d'essence est produit pour une marque donnée) ou la station-service où elle a été achetée (si des échantillons sont prélevés dans les stations-service chaque fois que leurs réservoirs sont remplis). Nous ne savons pas si des adversaires étatiques ont accès à de telles bases de données.³⁶

Dispositifs incendiaires

Un dispositif incendiaire est un assemblage d'éléments ou de matériaux conçu pour être laissé sur les lieux d'un incendie afin de contribuer à déclencher, accélérer, propager ou retarder le feu. Les dispositifs incendiaires vont des simples cocktails Molotov aux dispositifs complexes à retardement équipés de minuterie électronique.

Comme les dispositifs incendiaires sont conçus pour être laissés sur les lieux d'un incendie, un adversaire peut récupérer leurs restes brûlés et les analyser afin de trouver des preuves susceptibles d'aider à identifier les incendiaires. Il est relativement courant que des dispositifs incendiaires échouent—qu'ils ne s'enflamment pas ou qu'ils s'enflamment mais brûlent beaucoup moins que prévu—et un adversaire peut alors récupérer les dispositifs intacts ou partiellement intacts et potentiellement trouver beaucoup plus de preuves que si les dispositifs n'avaient pas échoué.

Les dispositifs incendiaires peuvent échouer à cause de :

- Un défaut inhérent à la conception ou à l'utilisation du dispositif. Par exemple, les cocktails Molotov ont généralement un taux d'échec élevé car ils ne se brisent souvent pas au contact de leur cible ou, s'ils se brisent, ils ne parviennent pas à enflammer suffisamment leur cible.
- Une manipulation brusque ou maladroite du dispositif pendant sa construction, son transport ou son installation. Une

³⁶ Une étude de 2020 des Pays-Bas mentionne brièvement « une base de données d'essence collectée à l'échelle nationale ».

- La composition chimique de l'accélérateur qui restait au fond du réservoir de carburant de la station-service lors de son dernier remplissage.³⁴

Un adversaire peut comparer les compositions chimiques de deux échantillons d'accélérateur pour déterminer la probabilité qu'ils proviennent de la même source. Il peut comparer :

- Un accélérateur à un autre. Ce type de comparaison est plus précis. Par exemple, il peut comparer une bouteille d'essence non enflammée trouvée sur les lieux d'un incendie à de l'essence trouvée chez un suspect.
- Des ILRs à un accélérateur. Ce type de comparaison est moins précis. Par exemple, il peut comparer des ILRs contenus dans des résidus d'incendie trouvés sur les lieux d'un incendie à un échantillon d'essence provenant d'une station-service.

Si un adversaire souhaite connaître la source d'un échantillon d'accélérateur (que nous appellerons « échantillon X ») mais ne dispose d'aucune piste particulière, il a deux options :

- Il peut collecter un grand nombre d'échantillons potentiellement correspondants et les comparer à l'échantillon X. Par exemple, il peut collecter des échantillons d'essence dans toutes les stations-service d'une région et les comparer à une bouteille d'essence non enflammée trouvée sur les lieux d'un incendie. Les adversaires étatiques ne font pas cela régulièrement.³⁵
- S'il a accès à une *base de données d'accélérateurs* (une base de données contenant des échantillons d'accélérateurs prélevés régulièrement dans une région donnée), il peut comparer l'échantillon X à tous les échantillons de la base de données. Par exemple, si l'échantillon X est une bouteille d'essence non enflammée trouvée sur les lieux d'un incendie, il pourrait

³⁴Les réservoirs des stations-service sont typiquement remplis tous les quelques jours, ou toutes les quelques semaines pour les stations avec moins de clients.

³⁵D'après une étude de 2023 des États-Unis, cela n'est « pas une pratique habituelle de la police scientifique ».

MESURES D'ATTÉNUATION

Dissimulation biométrique (#4) : Un adversaire peut identifier les caractéristiques d'un échantillon d'écriture pour identifier son auteur·e. Pour contrer ça, si tu écris un texte incriminant et que tu veux masquer ton écriture :

- Si tu n'as pas besoin de cacher que tu masques ton écriture, tu peux prendre autant que possible des mesures suivantes :
 - Tiens l'instrument d'écriture d'une manière inhabituelle. Par exemple, si tu tiens habituellement un stylo dans ta main droite, tiens-le plutôt dans ta main gauche.
 - Utilise un style d'écriture qui produit des caractères génériques plutôt qu'uniques. Par exemple, utilise une écriture scripte majuscule plutôt qu'une écriture cursive.
 - Attends quelques secondes entre chaque caractère pour éviter de retomber inconsciemment dans tes habitudes d'écriture.
 - Écris un texte le plus court possible.
- Si tu as besoin de cacher que tu masques ton écriture, tu peux utiliser une écriture qui a l'air naturelle mais n'a pas les caractéristiques de ton écriture normale. C'est difficile et peut demander des années d'entraînement.

OPÉRATIONS RÉPRESSIVES

Scripta Manent (#5) : Des échantillons écrits de plusieurs des accusé·e·s (dont des notes saisies pendant des perquisitions et des lettres écrites depuis la prison) ont été comparés aux adresses écrites sur des colis piégés qui n'ont pas explosé, dans le but de relier les accusé·e·s aux attaques.²⁵

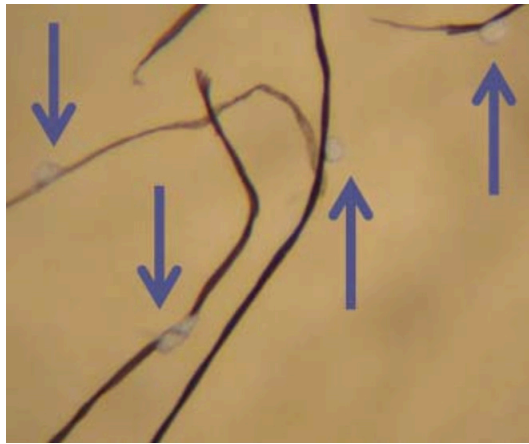
Opération de 2019-2020 contre Mónica et Francisco (#5) : Les étiquettes sur les deux colis piégés sont restées intactes—l'une parce que le colis n'a pas explosé, et l'autre malgré l'explosion du colis.⁷ Les signatures manuscrites sur les étiquettes ont été

²⁵<https://lib.anarhija.net/library/operation-scripta-manent-in-italy-2016-2019#toc15>

comparées et correspondaient. Cela a montré que les colis avaient été envoyés par la même personne.

Répression du premier incendie de Jane's Revenge (#5) : Une comparaison entre le graffiti en écriture cursive laissé sur le lieu de l'action et des graffiti dans le même style faits quelques mois plus tard lors d'une manifestation ont aidé à identifier la personne.¹⁷

3.18.3. Autres traces physiques



Goutelettes de peinture en spray adhérant aux fibres d'une veste, observées sous microscope (grossissement ~75x). En utilisant une bombe de peinture en spray, il est probable que des gouttelettes de peinture issues de la vaporisation tombent sur les surfaces à proximité.

Les autres traces physiques sont les petits fragments de preuves physiques qui sont transférés entre des objets, des personnes, et l'environnement. Ces traces peuvent être prélevées et analysées pour établir des liens entre des objets, des personnes, et des endroits.

Ces traces physiques peuvent être :

- Des fragments de matière. Par exemple de la boue sur la semelle d'une chaussure ou des éclats de verre provenant d'une fenêtre brisée.

Analyse des résidus d'incendie

L'analyse des résidus d'incendie est la collecte et l'analyse de résidus d'incendie—d'objets qui ont brûlé dans un incendie. Un adversaire peut prélever des échantillons de résidus d'incendie sur les lieux de l'incendie et les analyser en laboratoire pour trouver des traces appelées résidus de liquide inflammable (*ignitable liquid residues*, ILRs), qui sont laissées quand des accélérateurs brûlent. Un adversaire peut utiliser des **chiens de détection (#1)** pour localiser des ILRs sur les lieux de l'incendie, facilitant la collecte de résidus d'incendie susceptibles de contenir des ILRs.

Un adversaire peut analyser un échantillon de résidus d'incendie pour déterminer :

- La présence d'ILRs dans l'échantillon. Cela peut indiquer que l'incendie était d'origine volontaire plutôt qu'accidentelle et qu'il a démarré là où l'échantillon a été prélevé.
- Le type d'accélérateur qui a laissé les ILRs dans l'échantillon : essence, gazole, pétrole, etc.

Comparaison d'accélérateurs

Un accélérateur peut avoir une composition chimique plus ou moins unique selon comment il a été produit, transporté et stocké. Prenons l'exemple de l'essence, un accélérateur fabriqué à partir de pétrole brut raffiné. La composition chimique de l'essence vendue à une station-service dépend de :

- Où et comment le pétrole brut a été extrait.
- Comment le pétrole brut a été raffiné.
- Quels produits chimiques ont été mélangés pour fabriquer l'essence.
- Quels additifs ont été ajoutés à l'essence. Les additifs peuvent varier selon la marque d'essence, bien qu'une même marque puisse également utiliser différents additifs selon la région et la période de l'année.

Un adversaire peut généralement déterminer facilement si un incendie est accidentel ou volontaire. Il est difficile de commettre un incendie volontaire et de le faire passer pour un accident aux yeux d'un adversaire compétent en science forensique appliquée aux incendies volontaires.

Enquête sur les lieux de l'incendie

L'enquête sur les lieux de l'incendie consiste à analyser les lieux de l'incendie à la recherche :

- De la source d'ignition qui a démarré le feu et du combustible enflammé par cette source. Par exemple, dans un incendie accidentel dans une maison la source d'ignition peut être une prise électrique dysfonctionnelle qui surchauffe et le combustible peut être un canapé placé contre la prise. Dans un incendie volontaire la source d'ignition peut être une allumette et le combustible peut être de l'essence ramenée par l'incendiaire.
- Des motifs laissés par le feu sur les murs, sols, plafonds, et objets. Ces motifs peuvent indiquer où le feu a pris et comment il s'est propagé. Par exemple, un feu qui démarre à la base d'un mur peut laisser un motif distinctif en forme de V sur le mur.
- De témoignages de personnes présentes sur les lieux et d'images de **vidéo-surveillance (#3)** des lieux de l'incendie avant, pendant, et après l'incendie.

Lorsqu'un incendie se déroulant à l'intérieur d'une pièce atteint une température suffisamment élevée—typiquement entre 500°C et 600°C—il atteint le point de *flashover* (embrasement). Pendant le flashover, la pièce est si chaude que toutes les surfaces inflammables prennent feu plus ou moins simultanément et le feu se répand rapidement à travers la pièce. Une fois qu'un incendie a atteint le flashover il est généralement significativement plus difficile pour un adversaire d'interpréter les motifs qu'il a laissés sur des murs et autres surfaces.

- Des empreintes laissées quand deux surfaces entrent en contact. Par exemple l'empreinte d'une chaussure dans la boue ou une coupure faite par un coupe-boulons dans une clôture.

Ces traces physiques peuvent être transférées :

- Avec contact. Par exemple, un vêtement touche une clôture et des fibres du vêtement sont transférées sur la clôture.
- Sans contact. Par exemple, une vitre est brisée et des éclats de verre s'envolent et sont transférés sur les vêtements de personnes à proximité.
- Via une chaîne de transferts, avec et/ou sans contact.

Un adversaire peut utiliser ces traces physiques pour :

- Analyser une trace trouvée sur le lieu d'une action pour obtenir des informations utiles. Par exemple, il peut analyser l'empreinte d'une chaussure laissée sur le lieu d'une action pour déterminer la taille et le modèle de la chaussure qui l'a laissée, et ensuite chercher des personnes qui ont des chaussures de cette taille et de ce modèle.
- Relier une trace trouvée sur le lieu d'une action à un objet. Par exemple, il peut déterminer s'il est probable que des fibres textiles trouvées sur une clôture viennent d'un vêtement qu'il a saisi chez toi lors d'une **perquisition (#1)**.
- Relier une trace trouvée sur un objet au lieu d'une action. Par exemple, il peut déterminer s'il est probable que des éclats de verre trouvés sur tes vêtements pendant ton arrestation viennent d'une fenêtre qui a récemment été brisée à proximité.
- Relier des traces trouvées sur différents lieux d'action. Par exemple, il peut déterminer si des marques de marteau trouvées sur différents lieux d'action ont été laissées par le même marteau, et donc si les actions ont probablement été menées par les mêmes personnes.

Ces autres traces physiques n'incluent pas les **empreintes digitales (p. 26)** et l'**ADN (p. 3)**, qui sont considérés comme des domaines différents de la science forensique.

Fibres

Quand un objet fait de fibres textiles—un vêtement, un sac, etc.—touche une surface, il peut laisser des fibres sur la surface. La probabilité qu'un objet laisse des fibres sur une surface et la quantité de fibres laissées dépend de l'objet, de la surface, et de la durée et du type de contact entre les deux.

Un objet fait de fibres textiles peut laisser des fibres plus ou moins uniques, selon l'objet et son processus de fabrication. Par exemple :

- Un pull en laine usé d'une couleur peu commune, fabriqué d'une manière peu commune, peut laisser un grand nombre de fibres relativement uniques.
- Un coupe-vent en nylon neuf d'une couleur commune, fabriqué d'une manière commune, peut ne pas laisser de fibres, ou seulement des fibres très génériques.

Un adversaire peut :

- Analyser des fibres pour déterminer le type d'objet qui les a laissées et, dans certains cas, sa marque et son modèle.
- Comparer des fibres à un objet en sa possession pour déterminer si l'objet a pu laisser les fibres.
- Comparer deux ensembles de fibres pour déterminer si elles ont pu être laissées par le même objet.

Voir Handbook of Trace Evidence Analysis²⁴ (*Manuel d'analyse des traces physiques*), chapitre « Fibers » (*Fibres*) pour une vue d'ensemble des fibres.

Empreintes de pas

Quand tu es pieds nus et que tes pieds touchent une surface, tu peux laisser des empreintes de pas sur la surface. Tu laisses généralement des empreintes de pas sur les semelles intérieures des chaussures que tu portes. Tu peux laisser des empreintes de pas en portant des chaussettes.

Un pied peut laisser une empreinte plus ou moins unique, selon le pied et la surface. Par exemple :

OPÉRATIONS RÉPRESSIVES

Affaire de l'association de malfaiteurs de Bure (#5) : Des empreintes digitales ont été prélevées sur des objets trouvés dans des perquisitions, dont un carnet, des feuilles de papier, des masques à gaz, des cocktails Molotov, et des récipients contenant de l'essence ou autres substances.¹¹ La grande majorité des empreintes digitales prélevées n'ont correspondu à personne. Certaines des empreintes digitales prélevées ont correspondu à des individus dans le Fichier automatisé des empreintes digitales (FAED).

Répression de l'attaque sur le siège de Clarín (#5) : Les empreintes digitales d'une des inculpés ont été retrouvées sur un cocktail Molotov qui avait été utilisé lors de l'attaque mais ne s'était pas brisé.³³

3.18.6. Incendie volontaire



Un enquêteur incendie inspectant les lieux d'un incendie.

La science forensique appliquée aux incendies volontaires (aussi connue sous le nom d'*investigations incendie*) est l'application de la science aux enquêtes sur des incendies volontaires. Cette discipline cherche à déterminer l'origine et la cause d'un incendie et, s'il est suspecté d'être volontaire, à rassembler des preuves susceptibles d'aider à identifier les incendiaires.

³³<https://notrace.how/documentation/clarin-case-file.pdf>

surfaces, comme le métal, la réaction entre la graisse des doigts et le métal peut laisser une empreinte dans la surface elle-même, de telle sorte que l'empreinte digitale reste identifiable même après avoir nettoyé la surface avec un chiffon imbibé d'acétone.

Bases de données d'empreintes digitales

Dans de nombreux pays, l'État a des bases de données d'empreintes digitales contenant les empreintes digitales de nombreux individus, souvent obtenues lors d'arrestations ou après des condamnations.

Autres types d'empreintes

Chez les humains, les paumes des mains et les orteils peuvent laisser des traces similaires aux empreintes digitales, qui peuvent être prélevées et analysées de la même manière. Dans certains contextes, les empreintes de paumes sont régulièrement prélevées et ajoutées aux bases de données d'empreintes digitales.

Voir aussi

Voir le sujet « Empreintes digitales ».³²

MESURES D'ATTÉNUATION

Gants (#4) : Tu peux porter des gants pour éviter de laisser des empreintes digitales sur les surfaces que tu touches.

Préparation minutieuse de l'action (#4) : Un adversaire peut utiliser la science forensique appliquée aux empreintes digitales pour collecter et analyser des empreintes digitales sur le lieu d'une action. Pour contrer ça, tu peux préparer minutieusement l'action pour que tous les outils que tu prévoies d'utiliser pendant l'action soient dépourvus d'empreintes digitales au cas où tu les perdes ou tu aies besoin de t'en débarrasser dans un endroit où ils pourraient être récupérés par un adversaire.

- Sur une surface dure et poussiéreuse, un pied peut laisser une empreinte très unique montrant les plis des doigts de pied, qui sont aussi uniques que les **empreintes digitales** (p. 26).
- Sur une surface molle comme du sable, un pied peut laisser une empreinte très générique montrant seulement le contour approximatif du pied.

Un adversaire peut :

- Analyser une empreinte de pas pour obtenir des informations sur la personne qui l'a laissée, comme la taille de ses pieds, une estimation de sa taille, et ce qu'elle faisait quand elle a laissé l'empreinte—est-ce qu'elle se tenait debout, marchait, courait, se retournait, etc.
- Comparer une empreinte de pas à un pied pour déterminer si le pied a laissé l'empreinte.
- Comparer deux empreintes de pas pour déterminer si elles ont été laissées par le même pied.

Voir *Examination and Interpretation of Bare Footprints in Forensic Investigations*²⁶ (*Examen et interprétation des empreintes de pied par la science forensique*) pour une vue d'ensemble des empreintes de pas.

Empreintes de chaussure

Quand tu portes des chaussures et que tes pieds touchent une surface, tu peux laisser des empreintes de chaussure sur la surface.

Une chaussure peut laisser une empreinte plus ou moins unique, selon la chaussure et la surface. Même des chaussures du même modèle produites en masse présentent de légères variations dues aux irrégularités du processus de fabrication et aux traces d'usure. Par exemple :

- Sur un parquet propre, une chaussure usée et sale peut laisser une empreinte très unique.

³²<https://notrace.how/resources/fr/#topic=fingerprints>

²⁶<https://notrace.how/documentation/examination-and-interpretation-of-bare-footprints-in-forensic-investigations.pdf>

- Sur un tapis, une chaussure neuve, propre et sèche peut ne pas laisser d'empreinte, ou seulement une empreinte très générique.

Un adversaire peut :

- Analyser une empreinte de chaussure pour déterminer la taille et le modèle de la chaussure et obtenir des informations sur la personne qui l'a laissée, comme la taille de ses pieds et une estimation de sa taille.
- Comparer une empreinte de chaussure à une chaussure en sa possession pour déterminer si la chaussure a laissé l'empreinte. Pour cela, il peut utiliser la chaussure pour créer des empreintes de référence et les comparer à l'empreinte suspecte.
- Comparer deux empreintes de chaussure pour déterminer si elles ont été laissées par la même chaussure.

Voir Footwear Impression Evidence: Detection, Recovery and Examination²⁴ (*Empreintes de chaussure : détection, prélèvement et examen*) pour une vue d'ensemble complète des empreintes de chaussure.

Marques d'outil

Les outils—coupe-boulons, ciseaux, marteaux, tournevis, etc.—peuvent laisser des marques sur les objets sur lesquels ils sont utilisés.

Un outil peut laisser une marque plus ou moins unique, selon l'outil, comment il est utilisé, et selon la surface. Même des outils du même modèle produits en masse présentent de légères variations dues aux irrégularités du processus de fabrication et aux traces d'usure. Par exemple :

- Un marteau en métal usé utilisé pour frapper avec force une plaque métallique faite d'un métal plus mou peut laisser une marque très unique.
- Un coupe-boulons tout neuf utilisé pour couper une clôture peut laisser une marque relativement générique.

3.18.5. Empreintes digitales



Les plis sur un doigt humain.

La science forensique appliquée aux empreintes digitales est la collecte, le stockage et l'analyse des traces laissées par les plis présents sur les doigts humains.

Collecte

Des empreintes digitales sont laissées sur les surfaces que tu touches par l'humidité et la graisse sur tes doigts, et peuvent être prélevées sur ces surfaces. Elles peuvent aussi être prélevées directement depuis tes doigts avec de l'encre ou d'autres substances (les doigts sont d'abord trempés dans l'encre, puis posés sur du papier, laissant des empreintes sur le papier), ou avec des scanners d'empreintes électroniques.

Analyse

Parce que les empreintes digitales sont presque uniques et sont stables au cours de la vie d'un individu, deux empreintes digitales peuvent être comparées pour déterminer si elles appartiennent au même individu.

Les empreintes digitales laissées sur des surfaces se dégradent avec le temps et sous certaines conditions (par exemple en contact avec de l'acétone), et doivent contenir une quantité suffisante de détails pour être utilisables pour une comparaison. Sur certaines

3.18.4. Balistique



Sur la gauche, une balle 9mm qui n'a pas été utilisée.
Sur la droite, une balle du même modèle qui a été utilisée.

La science forensique appliquée à la balistique (aussi connue sous le nom de *balistique judiciaire*) est l'application de la science aux enquêtes sur les armes à feu et les balles. Quand une balle est tirée depuis une arme à feu, l'arme laisse des marques microscopiques sur la balle et sa douille. Ces marques sont des sortes d'empreintes digitales balistiques.

Quand un adversaire récupère une balle, des experts balistiques peuvent tirer avec l'arme à feu d'un suspect puis comparer les marques sur la balle récupérée aux marques sur la balle qu'ils ont tiré. Les douilles sont comparées de la même façon.

MESURES D'ATTÉNUATION

Achats anonymes (#4) : Un adversaire peut utiliser la science forensique appliquée à la balistique pour relier une arme à feu ou une balle à un vendeur, et de là à l'identité de la personne qui a acheté l'arme ou la balle. Pour contrer ça, tu peux acheter des armes à feu et des balles anonymement, par exemple grâce à des connexions à des réseaux de crime organisé ou à la fraude.

Cachette ou planque (#4) : Un adversaire a besoin d'avoir accès à une arme à feu pour faire une analyse balistique de l'arme. Pour contrer ça, tu peux stocker l'arme à feu dans une cachette ou une planque.

Un adversaire peut :

- Analyser une marque pour déterminer le type d'outil qui l'a laissée.
- Comparer une marque à un outil en sa possession pour déterminer si l'outil a laissé la marque. Pour cela, il peut utiliser l'outil pour créer des marques de références et les comparer à la marque suspecte.
- Comparer deux marques pour déterminer si elles ont été laissées par le même outil.

Voir aussi :

- PRISMA,²⁷ section « Tool Traces » (*Marques d'outil*) pour un aperçu rapide des marques d'outil.
- Color Atlas of Forensic Toolmark Identification²⁴ (*Atlas couleur de l'identification des marques d'outil par la science forensique*) pour une vue d'ensemble complète des marques d'outil.

Verre

Quand du verre se casse, il produit des éclats de différentes tailles.

Un objet en verre (par exemple une fenêtre, une bouteille) produit des éclats plus ou moins uniques quand il se casse, selon comment, où et quand il a été produit. Par exemple :

- Deux objets en verre de modèles différents, ou produits dans des usines différentes, ou produits dans la même usine à plusieurs semaines d'intervalle, peuvent produire des éclats qui peuvent être distingués en analysant leurs propriétés, y compris leurs indices de réfraction²⁸ et leurs éléments chimiques.²⁹
- Deux objets en verre du même modèle, produits dans la même usine la même semaine, peuvent produire des éclats impossibles à distinguer.

²⁷<https://notrace.how/resources/fr/#prisma>

²⁸https://fr.wikipedia.org/wiki/Indice_de_réfraction

²⁹https://fr.wikipedia.org/wiki/Élément_chimique

Un adversaire peut comparer deux éclats de verre pour déterminer la probabilité qu'ils viennent du même objet.

Voir Handbook of Trace Evidence Analysis²⁴ (*Manuel d'analyse des traces physiques*), chapitre « Interpretation of Glass Evidence » (*Interprétation des traces de verre*) pour une vue d'ensemble des traces de verre.

Traces d'accélération

Les traces d'accélération sont abordées dans la technique **Science forensique : Incendie volontaire** (p. 28).

Autre

Voici d'autres types de traces physiques :

- Les poils (et cheveux) humains et animaux. Les poils peuvent tomber d'un corps à tout moment. Les poils peuvent révéler diverses informations à propos de leur propriétaire, y compris, dans certains cas, son ADN (p. 3). Voir Handbook of Trace Evidence Analysis²⁴ (*Manuel d'analyse des traces physiques*), chapitre « Forensic Hair Microscopy » (*Microscopie forensique des poils*) pour une vue d'ensemble des poils.
- La peinture. Un objet peint peut laisser des traces de peinture sur une surface qu'il touche. Une trace de peinture peut révéler des informations sur l'objet qui l'a laissée. Voir Handbook of Trace Evidence Analysis²⁴ (*Manuel d'analyse des traces physiques*), chapitre « Paints and Polymers » (*Peintures et polymères*) pour une vue d'ensemble de la peinture.

MESURES D'ATTÉNUATION

Achats anonymes (#4) : Un adversaire peut utiliser des traces physiques pour relier des objets au lieu d'une action. Pour contrer ça, tu peux acheter anonymement les objets utilisés lors de l'action.

Cachette ou planque (#4) : Un adversaire peut utiliser des traces physiques pour relier des objets au lieu d'une action. Pour contrer ça, après l'action tu peux stocker dans une cachette ou une planque

les objets qui sont trop chers pour t'en débarrasser après chaque action.

Préparation minutieuse de l'action (#4) : Un adversaire peut utiliser des traces physiques pour relier des objets au lieu d'une action. Pour contrer ça, après l'action, tu peux prévoir de :

- Te débarrasser des objets que tu as utilisés lors de l'action.
- Si un objet est trop cher pour t'en débarrasser après chaque action, le stocker dans une **cachette ou une planque (#4)**.
- Si un outil est trop cher pour t'en débarrasser après chaque action, le modifier pour qu'un adversaire ne puisse pas le relier à des traces qu'il a pu laisser sur le lieu de l'action. Par exemple, tu peux te débarrasser du disque d'une disqureuse.

Tenue anonyme (#4) : Un adversaire peut utiliser des traces physiques pour relier des vêtements au lieu d'une action. Pour contrer ça, tu peux porter une tenue anonyme, et en particulier te débarrasser de la tenue après l'action.

OPÉRATIONS RÉPRESSIVES

Opération contre Jeff Luers (#5) : Lors de la perquisition du garde-meubles, la police a trouvé une pince coupante correspondant aux coupures faites dans la clôture du lieu de la tentative d'incendie de mai.³⁰

Opération contre Ruslan Siddiqi (#5) : Les enquêteurs ont trouvé des traces de pneus de vélo près du site de l'attaque à l'explosif contre le train.¹⁹ Cela a contribué à la théorie que la personne ayant mené l'attaque s'était déplacée à vélo.

Affaire du 8 décembre (#5) : Pendant les perquisitions, plusieurs objets (gazinière, poêles, gants, spatules) ont été analysés pour y chercher des traces de produits pouvant servir à fabriquer des explosifs.³¹

³⁰<https://courtlistener.com/opinion/2627996/state-v-luers>

³¹https://web.archive.org/web/20250615210912/https://soutien812.blackblogs.org/wp-content/uploads/sites/1922/2023/11/CompteRenduProces_A4.pdf