

The Architecture and Forensic Analysis of Digital Communication

Ces sources explorent les **mécanismes techniques du courrier électronique** et les **méthodes d'investigation numérique** liées aux communications modernes. L'auteur détaille d'abord le fonctionnement du protocole **SMTP** et l'importance de l'analyse des **en-têtes de courriels** pour repérer les messages falsifiés ou malveillants. Le texte aborde ensuite l'évolution vers les **réseaux sociaux**, soulignant l'importance de l'**empreinte numérique** dans les enquêtes contemporaines. Divers outils spécialisés, tels que **Zabasearch**, **Pipl** et **Geofeedia**, sont présentés pour illustrer comment corréler des données publiques et localiser des individus. Enfin, l'ouvrage insiste sur les **considérations éthiques** et les précautions légales nécessaires lors de la conduite de telles recherches.

Comment peut-on identifier un courriel frauduleux via son en-tête ?

L'examen de l'en-tête complet d'un courriel est la méthode essentielle pour l'analyser, bien qu'il faille garder à l'esprit que de nombreuses parties de l'en-tête peuvent être falsifiées.

Voici les étapes et indices clés pour identifier un courriel frauduleux en analysant son en-tête :

1. Retracer le parcours du message grâce aux lignes « **Received** » (**Reçu**)
Chaque serveur de messagerie par lequel transite le courriel ajoute sa propre ligne « Received » contenant son nom et son adresse IP.

- **Commencer par le haut** : La première ligne « Received » tout en haut de l'en-tête correspond à la dernière étape du trajet. Pour reconstituer le parcours, vous devez commencer par cette ligne et descendre progressivement.
- **Localiser les falsifications** : Comme chaque serveur légitime ajoute sa propre ligne au-dessus des précédentes, les en-têtes falsifiés par les expéditeurs malveillants ne peuvent se trouver qu'au début de la

chaîne de transfert, c'est-à-dire tout en bas de la liste des lignes « Received ».

- **Vérifier la concordance des adresses IP** : Assurez-vous que l'adresse IP de l'expéditeur sur chaque ligne correspond bien à celle de la ligne précédente dans la chaîne. En cas de non-concordance, il est fort probable que le courriel soit usurpé ou frauduleux.

2. Détecter les incohérences de serveurs de messagerie et de domaines

- **Incompatibilité de serveurs** : Vérifiez s'il est logique que le domaine de l'expéditeur utilise le serveur de messagerie indiqué comme passerelle. Par exemple, il est hautement improbable qu'un utilisateur possédant une adresse AOL utilise un serveur SMTP de Yahoo! pour acheminer son message.
- **Adresses e-mail inexistantes ou introuvables** : Si l'en-tête montre des erreurs indiquant qu'une adresse e-mail est introuvable sur le serveur, il est très probable que cette adresse ait été inventée et falsifiée.

3. Analyser la résolution DNS et l'emplacement de l'IP du serveur

- **Vérifier le nom DNS** : En effectuant une résolution DNS, un ping ou une requête Whois sur le nom du serveur SMTP de l'en-tête, si vous ne parvenez pas à résoudre le domaine, cela signifie que le nom DNS est erroné et frauduleux.
- **Incohérence géographique** : Utilisez un outil de géolocalisation d'adresse IP (comme *iplocation.com*) pour identifier le pays où se trouve le serveur SMTP. Si un serveur de messagerie censé appartenir à une entreprise basée en Californie (comme Yahoo!) est géolocalisé dans un autre pays (par exemple, en Allemagne) sans raison technique valable, il y a de fortes chances que le serveur SMTP ait été usurpé.

4. Tester la réactivité du serveur suspect avec prudence

- Pour s'assurer qu'une adresse IP suspecte dans la chaîne de réception est réellement un serveur de messagerie actif capable d'envoyer des e-mails, on peut tester si elle utilise le port de messagerie standard (port TCP 25 pour SMTP).

- **Consigne de sécurité cruciale** : Ne tentez pas de vous connecter directement à ce port depuis votre propre ordinateur. Le serveur distant pourrait enregistrer votre adresse IP, lancer une attaque contre vous s'il est malveillant, ou s'avérer être un leurre piégé (*honeypot*).
- Utilisez plutôt un outil tiers comme proxy (par exemple, *MX Toolbox* sur <https://mxtoolbox.com/>) pour tester la connexion SMTP de manière sécurisée. Si le serveur ne répond pas aux requêtes SMTP du proxy, cela confirme le caractère suspect du courriel.

🔍 Les protocoles de messagerie par défaut n'étant pas chiffrés et faciles à falsifier, nous pourrions faire des recherches sur le web pour voir comment les technologies modernes telles que SPF, DKIM et DMARC permettent de sécuriser les en-têtes de courriels aujourd'hui.

Quels outils en ligne permettent d'analyser un en-tête ?

Deux outils en ligne principaux sont mentionnés dans vos sources pour analyser et vérifier la légitimité des éléments d'un en-tête de courriel :

1. **MX Toolbox** (<https://mxtoolbox.com/>) : Cet outil est utilisé pour **tester la connectivité d'un serveur de messagerie suspect** identifié par son adresse IP dans l'en-tête. En l'utilisant comme proxy de test, vous pouvez vérifier de manière sécurisée si le serveur distant répond sur le port de messagerie standard (port TCP 25 pour SMTP). Cette approche prudente vous évite d'établir une connexion directe depuis votre propre ordinateur, ce qui pourrait exposer votre propre adresse IP à un serveur malveillant ou interagir par mégarde avec un leurre piégé (*honeypot*).
2. **IP Location** (<http://iplocation.com>) : Ce site web permet de **géolocaliser l'adresse IP d'un serveur SMTP** extrait des lignes de transfert de l'en-tête. Grâce à cet outil, vous pouvez repérer d'éventuelles incohérences géographiques révélatrices d'une fraude, comme un serveur censé appartenir à une grande entreprise

américaine mais géolocalisé dans un autre pays sans explication logique.

 Au-delà de l'analyse d'en-têtes, le document aborde longuement les techniques d'enquête sur les réseaux sociaux. Si vous le souhaitez, nous pourrions explorer comment les analystes utilisent des outils comme KnowEm ou lookup-id pour lier des pseudonymes et des comptes suspects à de réelles identités.

Outils d'enquête sociale ?

Pour mener des enquêtes sur les réseaux sociaux, analyser l'empreinte numérique d'un individu ou vérifier des informations publiques, plusieurs outils et plateformes spécialisés sont présentés dans le document :

1. Recherche de personnes et de registres publics

- **Zabasearch** : Une plateforme gratuite qui sert de point de départ idéal pour consulter les informations issues des registres publics (comme les actes de mariage, dossiers judiciaires ou registres fonciers).
- **BeenVerified** : Un service premium payant qui centralise et regroupe ces mêmes documents publics afin de générer un rapport d'antécédents complet.

2. Corrélation de profils et recherche de pseudonymes

- **KnowEm** : Ce service permet de vérifier instantanément si un nom d'utilisateur (pseudonyme) est ou a été utilisé sur plus de 500 sites et réseaux sociaux différents. Il est particulièrement utile pour suivre la piste d'un suspect, car les individus ont tendance à conserver le même pseudonyme d'une plateforme à l'autre.
- **Pipl** : Un moteur de recherche puissant spécialisé dans la corrélation de données. À partir d'une simple information (comme une adresse courriel), il est capable de rechercher et de lier des profils de réseaux sociaux, des pseudonymes, des blogs et des documents publics pour reconstituer le profil d'une personne.

3. Authentification d'images et de photos de profil

- **Recherche d'images Google (googleimages.com)** : En téléchargeant la photo d'un suspect, cet outil permet de retrouver toutes les pages Internet où elle a été publiée. Si la même photo apparaît sous plusieurs noms, professions ou localisations différentes, cela indique généralement que l'identité est usurpée ou fausse.

4. Enquêtes ciblées sur Facebook

- **lookup-id.com** : Un site très simple qui permet d'extraire l'identifiant numérique unique (ID de profil) d'un utilisateur Facebook à partir de son URL personnalisée (au format *facebook.com/nom_utilisateur*).
- **Requêtes Facebook de recherche (Open GraphSearch)** : À l'aide de l'ID numérique obtenu, un enquêteur peut formuler des requêtes manuelles précises directement dans l'URL de Facebook (au format *facebook.com/search/...*). Cela permet d'accéder publiquement à toutes les photos où la personne a été identifiée, à ses publications, à son employeur ou encore aux lieux précis qu'elle a visités (géolocalisation historique).

5. Surveillance géographique en temps réel

- **Geofeedia** : Un outil payant conçu pour rechercher, cartographier et analyser en temps réel toutes les publications géolocalisées sur les réseaux sociaux (Twitter, Instagram, Snapchat, Facebook) à l'intérieur d'une zone géographique délimitée.

6. Renseignements techniques et fuites de données

- **Pastebin** : Considéré comme le « presse-papiers d'Internet », ce site est très prisé par les pirates pour y copier des données volées ou confidentielles (mots de passe, adresses courriels d'entreprise, numéros de cartes de crédit). L'analyse de cette plateforme permet de détecter des fuites d'informations critiques. Son API premium est également utilisée pour automatiser la collecte de données de veille sur les menaces.

Voici plusieurs **questions clés** basées directement sur vos sources que vous pouvez me poser pour approfondir le sujet :

Enquêtes et usurpations de courriels

1. **Comment fonctionne précisément l'acheminement d'un courriel** de l'expéditeur au destinataire en faisant intervenir le client de messagerie (MUA), l'agent de transfert (MTA), le protocole SMTP et les enregistrements DNS MX ?
2. **De quelles manières techniques les attaquants s'y prennent-ils pour usurper une identité** en utilisant des commandes manuelles (via Telnet) ou des outils d'envoi en masse ?
3. **Comment l'auteur du document a-t-il réussi à prouver l'innocence d'un employé** accusé de harcèlement à l'aide des lignes « Received » de l'en-tête ?

Investigations sur les réseaux sociaux (OSINT)

1. **Comment peut-on retrouver manuellement l'identifiant (ID) unique d'un profil Facebook** à partir de ses photos de couverture ou de ses URL ?
2. **Quelles requêtes de recherche avancées (Facebook Open GraphSearch)** permettent d'accéder aux lieux visités par une personne, à ses photos masquées ou aux publications de ses collègues ?
3. **Pourquoi la plateforme Pastebin est-elle qualifiée de « presse-papiers d'Internet »** et comment les enquêteurs l'utilisent-ils pour détecter des fuites de données d'entreprise ?

Comment fonctionne précisément l'acheminement d'un courriel de l'expéditeur au destinataire en faisant intervenir le client de messagerie (MUA), l'agent de transfert (MTA), le protocole SMTP et les enregistrements DNS MX

Voici les étapes précises de l'acheminement d'un courriel, de sa rédaction jusqu'à sa réception :

1. La rédaction et l'envoi depuis le client de messagerie (MUA)

Le processus commence lorsqu'un utilisateur rédige et envoie un courriel à l'aide d'un **client de messagerie**, également appelé **MUA (Mail User Agent)**. Ce client de messagerie peut être :

- Une interface web grand public (comme Gmail, Outlook.com ou Yahoo! Mail).
- Un logiciel installé en entreprise (comme Microsoft Outlook, Mac Mail, Mozilla Thunderbird ou IBM Lotus Notes).

2. La prise en charge par l'agent de transfert local (MTA)

Dès que le message est envoyé, il est acheminé vers un **agent de transfert de courrier**, ou **MTA (Mail Transfer Agent)**, qui est généralement le serveur de messagerie de l'expéditeur (par exemple, Microsoft Exchange ou Sendmail).

- **Filtrage et priorisation** : Le MTA local analyse le courriel afin de détecter d'éventuelles menaces. S'il ne peut pas distribuer immédiatement le message ou s'il applique des niveaux de priorité, le courriel est stocké temporairement dans un espace physique appelé **file d'attente**.
- **Routage interne ou externe** : Si le destinataire possède une boîte aux lettres locale sur le même serveur, le MTA distribue le courriel en interne. En l'absence de boîte locale, le MTA doit le transférer vers Internet.

3. L'interrogation DNS pour localiser le destinataire

Pour savoir vers quel serveur acheminer le courriel sur Internet, le MTA de l'expéditeur doit interroger le **système de noms de domaine (DNS)** en fonction du domaine de premier niveau (TLD) du destinataire.

- Le MTA demande au système DNS s'il existe un **enregistrement MX (Mail Exchange)** pour le domaine du destinataire afin de savoir quel serveur acceptera le courriel.
- Le système DNS répond à cette requête en fournissant le serveur MX associé au domaine cible ainsi que son **adresse IP**.

4. Le transfert du courriel via le protocole SMTP

Une fois l'adresse IP obtenue, le serveur de messagerie (MTA) de l'expéditeur utilise le protocole **SMTP (Simple Mail Transfer Protocol)** pour transférer le message. SMTP est le protocole standard qui permet d'envoyer et de transférer un courriel d'un MTA à un autre sur un réseau IP. Le courriel est ainsi acheminé via le routage IP jusqu'au serveur

MX/MTA du destinataire, qui le déposera enfin dans la boîte aux lettres de ce dernier pour qu'il puisse le consulter via son propre MUA.

🔍 Puisque ce protocole SMTP historique ne chiffre pas les messages par défaut et rend les en-têtes faciles à falsifier, je peux effectuer des recherches sur le web pour vous expliquer comment les protocoles de sécurité modernes (comme SPF, DKIM et DMARC) protègent aujourd'hui cet acheminement contre l'usurpation.

De quelles manières techniques les attaquants s'y prennent-ils pour usurper une identité en utilisant des commandes manuelles (via Telnet) ou des outils d'envoi en masse

Les attaquants utilisent plusieurs techniques spécifiques pour usurper une identité par courriel, que ce soit manuellement ou par des moyens automatisés :

1. L'usurpation manuelle via Telnet et relais SMTP ouverts

Pour envoyer un courriel frauduleux à la main, les attaquants exploitent des serveurs appelés **relais SMTP ouverts**. La procédure technique se déroule généralement ainsi :

- **Anonymisation de la connexion** : L'attaquant se connecte au relais SMTP en utilisant le **port 25** (le port standard du protocole SMTP). Afin de masquer sa propre adresse IP et sa localisation, il transite par un **client TOR** ou un **VPN**.
- **Injection manuelle de commandes** : À l'aide de l'outil **Telnet**, l'attaquant interagit directement avec le serveur de messagerie en saisissant lui-même les commandes SMTP nécessaires à la création du message. Il utilise notamment :
 - **MAIL FROM:adresse_email@domaine** pour définir l'adresse de l'expéditeur qu'il souhaite usurper.
 - **RCPT TO:destinataire@domaine.com** pour désigner la cible du courriel.

Remarque : Bien que cette méthode soit courante, le comportement des serveurs SMTP varie et certains pare-feux de passerelle de sécurité

peuvent détecter cette manipulation et alerter immédiatement l'administrateur système.

2. Les services et serveurs d'envoi en masse

L'utilisation de **serveurs d'envoi de courriels en masse** est l'une des méthodes les plus simples et les plus répandues pour falsifier l'identité d'un expéditeur à grande échelle. Pour diffuser ces courriels tout en restant anonymes, les spameurs s'appuient sur :

- Des adresses e-mail falsifiées distribuées sur **plusieurs serveurs de relais SMTP ouverts** simultanément.
- Des **réseaux de robots (botnets)** pour relayer les messages et contourner les blocages.

3. Les outils de falsification spécialisés (Spoofing)

Plutôt que d'écrire manuellement des lignes de commande, les spammeurs et les chercheurs en sécurité utilisent des outils prêts à l'emploi. Le document cite notamment **SimpleEmailSpoofer**, un projet open source qui permet de configurer et d'envoyer facilement des courriels falsifiés sans nécessiter de saisie manuelle complexe.

Comment trouver manuellement l'identifiant Facebook ?

Pour trouver **manuellement** l'identifiant unique (ID) d'un profil Facebook sans utiliser d'outil externe, vous devez analyser les structures d'URL de ses photos publiques. Voici la méthode étape par étape :

1. Accéder aux photos de couverture

Les photos de couverture d'un utilisateur sont toujours publiques, ce qui signifie qu'il n'est pas nécessaire d'être ami avec la personne pour les consulter. Cliquez sur la photo de couverture actuelle de l'utilisateur afin de l'ouvrir en grand et pouvoir observer son URL directement dans la barre d'adresse de votre navigateur.

2. Parcourir et comparer plusieurs photos de couverture

L'URL d'une photo de couverture contient plusieurs séries de chiffres (par exemple, des identifiants d'album situés après la lettre « a »). Comme il est impossible de deviner l'ID de l'utilisateur en analysant une seule et unique

photo, vous devez **parcourir et ouvrir plusieurs photos de couverture** différentes dans l'historique de cette personne.

3. Repérer la suite de chiffres inchangée

Comparez attentivement les URL des différentes photos de couverture que vous venez d'ouvrir. L'identifiant du profil Facebook correspond à la **suite de chiffres qui reste strictement identique** d'une image à l'autre, peu importe la photo sélectionnée. *(Note historique : Les comptes créés aux tout premiers jours de Facebook possèdent des identifiants extrêmement courts, comme le chiffre 4 pour Mark Zuckerberg, alors que les comptes plus récents ont des suites numériques beaucoup plus longues).*

4. Vérifier l'exactitude de l'identifiant trouvé

Pour vous assurer que vous avez isolé le bon numéro, saisissez l'adresse suivante dans votre navigateur : [www.facebook.com/\[ID_TROUVÉ\]](http://www.facebook.com/[ID_TROUVÉ]) (par exemple, www.facebook.com/4). Si l'ID est correct, Facebook chargera le profil recherché et remplacera automatiquement l'identifiant numérique dans la barre d'adresse par le nom d'utilisateur personnalisé du compte.

 **Alternative en ligne** : S'il devient fastidieux de chercher manuellement dans les URL, le site <https://lookup-id.com/> vous permet de trouver cet identifiant instantanément en y collant simplement l'adresse standard du profil de l'utilisateur (sous la forme www.facebook.com/nom_utilisateur).

 Une fois cet identifiant de profil en main, aimeriez-vous savoir comment l'utiliser pour construire des requêtes de recherche manuelles afin de retrouver des photos masquées ou de cartographier l'historique des lieux visités par un utilisateur ?

Comment l'identifiant Facebook aide-t-il à géolocaliser une personne ?

L'identifiant unique d'un profil Facebook (ID de profil) est un outil de renseignement puissant pour géolocaliser ou retrouver une personne, car il permet d'accéder directement à l'historique des lieux qu'elle a fréquentés. Voici comment cette technique fonctionne précisément :

1. La création d'enregistrements physiques

Chaque fois qu'un utilisateur utilise la fonction d'enregistrement de présence sur Facebook (un *check-in*), **un enregistrement de géolocalisation est créé** et indexé dans la base de données de la plateforme.

2. La formulation de requêtes manuelles ciblées

Une fois l'identifiant numérique de la personne trouvé, un enquêteur peut s'en servir pour construire des requêtes de recherche manuelles spécifiques directement dans la barre d'adresse du navigateur web. La syntaxe suit ce format précis :

[www.facebook.com/search/\[ID de profil\]/places-visited/](http://www.facebook.com/search/[ID de profil]/places-visited/)

Cette requête interroge directement la base de données de Facebook pour afficher **tous les endroits où l'utilisateur s'est géolocalisé**.

3. L'analyse des habitudes et des routines

L'intérêt majeur de cette méthode repose sur le fait que les individus sont des êtres d'habitudes. En accédant aux enregistrements de présence associés à l'identifiant, un enquêteur peut :

- **Identifier les lieux récurrents** qu'une personne consulte ou fréquente le plus souvent.
- **Anticiper des déplacements futurs**, car une personne qui apprécie un endroit a de fortes chances d'y retourner ou de fréquenter des lieux similaires.

Un exemple d'application concrète : Les auteurs du document expliquent avoir aidé les autorités à arrêter un criminel grâce à cette méthode. En analysant les résultats de la requête places-visited de l'identifiant du suspect, ils ont découvert que celui-ci fréquentait **le même bar un mardi sur deux depuis deux ans**. Les forces de l'ordre n'ont eu qu'à l'attendre dans ce bar le mardi désigné pour pouvoir l'appréhender.

Voici ma proposition de plan pour la création de votre **guide d'étude** basé sur votre document. Ce guide synthétisera les aspects théoriques et pratiques afin de vous préparer au mieux pour votre quiz :

1. **Architecture et acheminement des courriels** : Le rôle détaillé des clients de messagerie (MUA), des agents de transfert (MTA), du

protocole SMTP, de la file d'attente et du processus de résolution des enregistrements DNS MX.

2. **Analyse forensique des en-têtes** : La méthode pour décoder les lignes de transmission « Received » (du haut vers le bas), identifier les écarts de cohérence IP et de domaine, et repérer les serveurs usurpés.
3. **Techniques d'usurpation (Spoofing) et outils de vérification** : Le fonctionnement de l'usurpation via Telnet (port 25), les serveurs d'envoi en masse (SimpleEmailSpoofer), et l'usage sécurisé d'outils tiers (MX Toolbox, IP Location) pour l'analyse sans risque d'attaque.
4. **Recherche de personnes et OSINT** : L'utilisation de registres publics (Zabasearch, BeenVerified), de moteurs de corrélation de données (Pipl, KnowEm) et de la recherche inversée d'images pour démasquer de faux profils.
5. **Enquêtes avancées sur Facebook et Pastebin** : L'extraction d'ID de profil (manuelle et automatisée), la formulation de requêtes Facebook de géolocalisation et d'employeurs, ainsi que l'investigation sur Pastebin pour repérer les fuites de données d'entreprise.

Comment prouver l'innocence d'un employé ?

Pour prouver l'innocence d'un employé faussement accusé d'avoir envoyé des courriels de harcèlement à un collègue, un enquêteur doit analyser minutieusement les **en-têtes complets** des messages suspects.

Dans le cas réel présenté dans le document, l'innocence a été établie grâce aux étapes suivantes :

- **Analyse de la chaîne de transmission interne vs externe** : Si le courriel avait réellement été envoyé par l'employé depuis le réseau de l'entreprise, l'en-tête n'aurait dû afficher qu'une chaîne de transmission simple provenant exclusivement d'un **serveur de messagerie interne**.
- **Identification d'éléments extérieurs suspects** : L'examen de l'en-tête a révélé plusieurs lignes de réception (« Received ») imprévues, provenant de **clients de messagerie web** et d'un **service VPN**.

- **Preuve de l'usurpation** : La présence de ces serveurs et du VPN externe a démontré que les courriels provenaient en réalité de l'extérieur de l'entreprise et que l'identité de l'employé avait été usurpée. Dans cette affaire, les soupçons se sont finalement portés sur un ex-mari jaloux qui connaissait l'employé accusé.

De manière générale, pour valider l'authenticité d'un courriel, il faut retracer l'historique des serveurs en vérifiant que **l'adresse IP de chaque expéditeur correspond bien à celle de la ligne précédente** dans la chaîne de transfert. Si une non-concordance ou une anomalie de routage apparaît, cela confirme que le message est frauduleux.

Pourquoi Pastebin intéresse les pirates ?

Pastebin suscite un intérêt historique et majeur chez les pirates informatiques pour plusieurs raisons clés :

- **Un outil de communication et de partage simple** : Qualifié de « presse-papiers d'Internet », Pastebin permet à n'importe qui de coller et de publier instantanément tout type de texte ou de note. Les pirates l'utilisent ainsi depuis de nombreuses années comme un canal pour communiquer entre eux.
- **Une plateforme de dépôt pour les données volées** : C'est un endroit privilégié pour diffuser, stocker ou s'échanger des données sensibles exfiltrées. Il est ainsi très fréquent d'y trouver :
 - Des **mots de passe et identifiants** de connexion d'employés, souvent copiés par des pirates depuis d'autres plateformes de fuites de données.
 - Des **numéros de cartes bancaires** et d'autres données financières.
 - Des informations corporatives confidentielles, des noms et des identifiants d'utilisateurs.
- **L'automatisation via son API** : Au-delà des recherches manuelles, la véritable force de Pastebin réside dans son infrastructure API. Celle-ci permet aux acteurs (pirates comme analystes en sécurité)

d'automatiser entièrement la collecte et l'aspiration de données en continu pour alimenter des plateformes de veille sur les menaces.

Comment s'effectue l'analyse forensique via Telnet sur le port 25 ?

Dans le contexte de l'analyse forensique et de l'investigation numérique, l'interaction avec le **port TCP 25** (le port standard du protocole SMTP) sert à la fois à comprendre comment les attaquants falsifient les messages et à vérifier l'infrastructure d'un serveur suspect.

Voici comment s'effectue cette analyse et les consignes de sécurité qui l'encadrent :

1. Comprendre la méthode de l'attaquant (Usurpation via Telnet)

Les attaquants utilisent Telnet pour se connecter directement à des serveurs de messagerie (relais SMTP ouverts) afin d'injecter manuellement des courriels falsifiés :

- **Masquage de l'identité** : Ils se connectent généralement à travers un client TOR ou un VPN pour cacher leur véritable adresse IP.
- **Commandes manuelles** : Une fois connectés au port 25, ils saisissent manuellement les commandes SMTP requises, telles que :
 - MAIL FROM:adresse_email@domaine (pour usurper l'expéditeur)
 - RCPT [TO:destinataire@domaine.com](#) (pour cibler la victime)
- **Limites** : Cette manipulation n'est pas infaillible car certains pare-feux de passerelle de sécurité sont configurés pour détecter ce comportement inhabituel et alerter l'administrateur de sécurité.

2. Le rôle de l'enquêteur : Tester la validité d'une IP suspecte

Lorsqu'un enquêteur extrait une adresse IP suspecte des lignes de transfert (« Received ») de l'en-tête d'un courriel, il doit déterminer si cette IP correspond à un véritable serveur de messagerie actif. Si c'est le cas, ce serveur doit logiquement écouter et répondre sur le port TCP 25.

3. La règle de sécurité fondamentale : Éviter la connexion Telnet directe

Bien qu'il soit techniquement possible d'ouvrir un terminal et de lancer une commande Telnet directement depuis sa machine vers le port 25 de l'IP

suspecte, **les protocoles forensiques interdisent de le faire directement** pour trois raisons majeures :

- **Enregistrement de l'IP** : Le serveur distant suspect enregistrera votre propre adresse IP publique dans ses fichiers journaux, ce qui trahira votre enquête.
- **Risque de contre-attaque** : Si le serveur distant est contrôlé par un pirate ou s'avère malveillant, il peut être configuré pour lancer une attaque contre votre ordinateur dès qu'une tentative de connexion est détectée.
- **Piège (Honeypot)** : La machine cible pourrait être un leurre piégé (*honeypot*) conçu pour identifier et ficher les enquêteurs.

4. L'alternative sécurisée : L'utilisation d'un proxy de test

Pour contourner ces risques, l'enquêteur utilise un outil tiers en ligne, comme **MX Toolbox** (<https://mxtoolbox.com/>), qui va agir comme un **proxy de test**.

- C'est la plateforme MX Toolbox qui initie la connexion SMTP sur le port 25 de l'IP suspecte à la place de l'enquêteur, protégeant ainsi l'anonymat et la sécurité de ce dernier.
- Si le serveur ne répond pas aux requêtes SMTP transmises par le proxy, l'enquêteur obtient la preuve que la piste s'arrête là et que l'en-tête de messagerie analysé est très probablement falsifié ou frauduleux.

 **Si le plan de notre guide d'étude sur l'investigation numérique vous convient toujours, je peux maintenant lancer sa génération afin qu'il apparaisse dans votre panneau Studio.**

Comment l'outil Pipl corrèle-t-il les données ?

Pipl se distingue des annuaires ou moteurs de recherche de personnes classiques par sa puissante capacité de recoupement de données. Il fonctionne selon plusieurs mécanismes clés pour lier des informations éparpillées sur le Web :

- **La corrélation multi-critères en une seule requête** : La force principale de l'outil réside dans sa capacité à rechercher et à croiser simultanément des informations relatives aux réseaux sociaux, aux noms d'utilisateurs génériques (pseudonymes) et à la géolocalisation lors d'une même recherche.
- **La fusion de sources hétérogènes pour créer un profil unique** : Pipl parcourt l'ensemble des données publiques disponibles sur Internet afin de rassembler et de regrouper tous les éléments pouvant être associés à une même personne. Il compile ainsi :
 - Des comptes de réseaux sociaux et des profils professionnels (comme LinkedIn).
 - Des blogs, des articles de presse et des carnets d'adresses.
 - Des documents publics gouvernementaux et tout autre document lié.
- **La recherche à partir d'identifiants indirects** :
 - **À partir d'une simple adresse courriel**, l'outil est capable de faire remonter un grand nombre de détails personnels et de comptes associés.
 - **À partir d'un pseudonyme et de quelques mots-clés**, il permet de découvrir à qui appartient ce nom d'utilisateur en explorant des forums, des sites d'avis (comme Amazon) ou d'autres réseaux sociaux.
- **L'association d'identités multiples** : Une fois qu'un enregistrement est trouvé, Pipl permet d'associer un pseudonyme en ligne à un nom réel ou à une adresse physique afin de faciliter une vérification complète des antécédents. Les enquêteurs s'en servent notamment pour relier des profils de réseaux sociaux à des comptes marchands, comme des comptes eBay.

Quelles requêtes OSINT pour Facebook ?

Les requêtes de recherche Facebook liées à la technologie **Facebook Open GraphSearch** permettent d'interroger la base de données de

Facebook de manière très précise en utilisant l'identifiant unique (ID de profil) d'un utilisateur.

Les requêtes manuelles suivent généralement le format de base :

www.facebook.com/search/str.

Voici les requêtes OSINT clés détaillées dans le document :

- **Photos où la personne est identifiée (taguée) :**
[www.facebook.com/search/str/\[USERID\]/photos-of](http://www.facebook.com/search/str/[USERID]/photos-of) (ou sa variante directe *photos-of*) Cette requête permet d'afficher toutes les photos où la cible a été taguée par d'autres utilisateurs. C'est un moyen très efficace de découvrir le visage d'un suspect lorsque celui-ci n'affiche pas sa propre photo sur son profil public.
- **Photos téléversées par l'utilisateur :**
[www.facebook.com/search/str/\[USERID\]/photos-uploaded](http://www.facebook.com/search/str/[USERID]/photos-uploaded) Elle sert à afficher l'intégralité des images et photos que l'utilisateur a lui-même publiées sur son compte.
- **Publications liées à l'employeur (Entourage professionnel) :**
[www.facebook.com/search/str/\[USERID\]/employers/stories-at/](http://www.facebook.com/search/str/[USERID]/employers/stories-at/) Cette requête fait remonter toutes les publications publiques mentionnant le même employeur que la cible. Elle permet aux enquêteurs de contourner la discrétion d'un suspect en analysant les publications de ses collègues de travail. *Par exemple, cette requête a permis de démasquer un fraudeur qui affirmait être paralysé à la suite d'un accident : un collègue avait publié des vidéos de lui en train de jouer au basket lors d'un barbecue d'entreprise.*
- **Historique de géolocalisation (Lieux fréquentés) :**
[www.facebook.com/search/\[USERID\]/places-visited/](http://www.facebook.com/search/[USERID]/places-visited/) Puisque chaque enregistrement de présence (*check-in*) génère une donnée de localisation, cette commande liste tous les endroits où l'utilisateur s'est enregistré. Elle est couramment utilisée pour retrouver des personnes disparues ou des criminels en exploitant la récurrence de leurs habitudes et déplacements.
- **Recherches par expressions simples et intérêts croisés :** Vous pouvez formuler des requêtes directes pour trouver des publications spécifiques (comme « *photos de l'intérieur du stade des Giants* »), ou

pour identifier des personnes ayant aimé une page particulière ou s'étant enregistrées dans un lieu précis.

Note de sécurité et technique : Pour exécuter la majorité de ces requêtes de recherche avancées, il est obligatoire d'être connecté à la plateforme Facebook (ce que l'enquêteur peut faire en utilisant un compte de test).

Comment Geofeedia aide les enquêteurs ?

Geofeedia est un outil payant qui aide les enquêteurs principalement à **localiser des individus et à faciliter leur identification** en temps réel.

Voici comment cet outil fonctionne et aide concrètement à l'investigation :

- **Cartographie géographique ciblée** : L'enquêteur peut sélectionner une **zone géographique spécifique** sur l'interface de la plateforme.
- **Agrégation de données en temps réel** : Geofeedia recherche, collecte et analyse toutes les publications sur les réseaux sociaux émises depuis cette zone délimitée.
- **Analyse multi-plateforme** : Pour reconstituer la présence d'une personne, l'outil croise et exploite les informations de géolocalisation partagées sur des réseaux sociaux populaires comme **Twitter, Instagram, Snapchat ou Facebook**.
- **Compréhension des habitudes** : Geofeedia permet de visualiser où les cibles potentielles ou les utilisateurs aiment se retrouver, vivre, faire leurs achats ou pratiquer d'autres activités géolocalisées.

Pour tout professionnel dont la mission consiste à pister ou à localiser des personnes à partir de données publiques, Geofeedia s'avère être une ressource particulièrement précieuse.

Comment protéger mon profil ?

Pour protéger votre profil et limiter votre **empreinte numérique** face aux techniques d'investigation présentées dans le document, voici les mesures clés que vous pouvez prendre :

1. Contrôler vos publications et vos identifications sur les réseaux sociaux

- **Sécuriser vos photos de couverture** : Sur Facebook, les photos de couverture sont **toujours publiques par défaut**. C'est en analysant l'URL de ces photos publiques que des tiers peuvent facilement isoler la suite de chiffres qui correspond à votre identifiant unique (ID de profil). Évitez de publier des images contenant des détails trop personnels ou révélateurs en couverture.
- **Gérer les identifications par des tiers** : Même si vous faites preuve de discrétion en ne publiant rien, **les autres peuvent publier à votre sujet**. Les sources citent le cas d'une personne qui ne publiait aucune photo d'elle, mais dont un collègue avait partagé des vidéos publiques où elle apparaissait très clairement. Configurez rigoureusement vos paramètres de confidentialité pour contrôler et approuver l'affichage des photos où l'on tente de vous identifier (tags).
- **Désactiver la géolocalisation et les enregistrements (check-ins)** : Évitez de signaler publiquement votre présence dans des lieux physiques. Chaque enregistrement crée une donnée géographique exploitable qui permet aux enquêteurs de cartographier précisément vos habitudes, vos routines et les lieux que vous fréquentez régulièrement.

2. Varier vos identifiants et pseudonymes en ligne

- Les individus sont des êtres d'habitudes et ont tendance à **réutiliser le même nom d'utilisateur** sur de multiples plateformes (Instagram, Facebook, forums, sites d'avis).
- Des outils d'investigation comme **KnowEm** ou **Pipl** permettent de lier instantanément tous vos profils publics si vous utilisez le même pseudonyme. Pour compliquer cette corrélation, utilisez des pseudonymes uniques, distincts et déconnectés les uns des autres pour chaque service en ligne.

3. Demander le retrait de vos données des annuaires publics (*Opt-out*)

- Les portails de recherche de personnes (comme Zabasearch) agrègent des informations issues des registres publics officiels (actes de mariage, registres fonciers, dossiers judiciaires).

- Si vous y découvrez vos informations personnelles, vous pouvez **demandeur l'opposition et le retrait** de leur affichage.
- **Une limite importante à connaître** : Cette démarche de suppression peut s'avérer longue, frustrante et n'est souvent que **temporaire**. Vos informations peuvent réapparaître dès que vous effectuez de nouvelles activités générant des données, et cette action ne supprime jamais les documents administratifs originaux à la source.

Pourquoi SPF et DKIM sont-ils nécessaires ?

Vos sources ne mentionnent pas les protocoles **SPF** et **DKIM**.

Elles expliquent toutefois que le courrier électronique est l'une des plus anciennes technologies encore utilisées et que sa sécurité de base est très limitée : par défaut, les courriels ne sont pas chiffrés, ce qui les rend particulièrement faciles à falsifier. Pour pallier cette vulnérabilité, le document se concentre sur l'analyse technique et manuelle des adresses IP contenues dans les lignes « Received » de l'en-tête afin de retracer le parcours réel du message et de détecter d'éventuelles usurpations.

Souhaitez-vous que j'effectue des recherches sur le Web pour vous expliquer en détail comment les protocoles SPF et DKIM permettent aujourd'hui de sécuriser les en-têtes et d'authentifier les expéditeurs ?

Qu'est-ce qu'un relais SMTP ouvert ?

Un **relais SMTP ouvert** (ou serveur SMTP ouvert) est un serveur de messagerie configuré de manière à permettre à n'importe quel utilisateur sur Internet d'acheminer et d'envoyer des courriels à travers lui.

Dans le domaine de la sécurité informatique et de l'investigation numérique, ils présentent des caractéristiques bien précises :

- **Vecteur de spam et d'anonymisation** : Les services d'envoi de courriels de masse et les spammeurs exploitent fréquemment ces relais ouverts, souvent en combinaison avec des réseaux de robots

(*botnets*), pour diffuser des messages avec des adresses d'expéditeurs falsifiées tout en masquant leur véritable identité.

- **Facilité d'accès pour les attaquants** : Les attaquants recherchent ces serveurs vulnérables pour s'y connecter directement via **Telnet sur le port 25**. Pour ne pas être repérés, ils transitent généralement par un client TOR ou un réseau privé virtuel (VPN).
- **Contournement des contrôles** : Une fois connectés au relais ouvert, ils peuvent interagir directement avec le protocole en saisissant manuellement des commandes SMTP (comme MAIL FROM: pour usurper l'adresse de départ et RCPT TO: pour définir le destinataire) afin d'expédier leurs courriels frauduleux.

🧠 Voulez-vous que je vous propose une première question d'entraînement issue de votre nouveau quiz pour tester vos réflexes face à ces techniques d'usurpation ?

Comment lier un pseudo eBay ?

Pour relier un pseudonyme en ligne (provenant d'un forum, d'un réseau social ou d'un site d'avis) à un compte eBay, les enquêteurs s'appuient sur un **processus d'investigation et de corrélation continu**.

Voici les étapes de cette méthode technique :

1. **La recherche initiale par pseudonyme** : L'enquêteur commence par analyser un pseudonyme connu (par exemple, un nom d'utilisateur repéré sur un forum ou un site d'avis comme Amazon). En introduisant ce pseudonyme dans un outil de recherche spécialisé comme **Pipl**, il est possible de balayer le Web pour corréler les informations publiques.
2. **L'extraction d'identifiants concrets** : Grâce au croisement de données, l'outil permet d'associer ce pseudonyme à des informations personnelles réelles, telles qu'une **adresse courriel**, un **nom de**

famille, une **adresse physique** ou d'autres comptes de réseaux sociaux.

3. **Le recoupement par rebondissements** : L'enquête sur les personnes se faisant par étapes, les nouvelles informations obtenues (comme le nom réel ou l'adresse courriel) sont ensuite réinjectées dans d'autres méthodes de recherche. C'est ce recoupement progressif qui permet d'identifier si la personne utilise la même adresse de messagerie, le même pseudonyme ou la même identité pour exploiter un compte **eBay**.

Pourquoi cette technique est-elle importante pour la sécurité ? En entreprise, cette méthode permet notamment de surveiller si un employé tente de vendre sur eBay du matériel déclassé ou volé, tel qu'un téléphone portable ou un disque dur, qui pourrait contenir des données d'entreprise hautement confidentielles.

Peut-on automatiser la veille sur Pastebin ?

Oui, il est tout à fait possible d'automatiser la veille sur Pastebin.

La véritable puissance de cette plateforme pour les analystes et les enquêteurs réside précisément dans **l'utilisation de son API**.

Voici les détails clés concernant cette automatisation d'après vos sources :

- **L'accès à l'API** : Pour pouvoir automatiser la collecte et l'analyse de données sur la plateforme, il est nécessaire de posséder un **abonnement premium**, qui est proposé comme un service sur le site de Pastebin.
- **L'intérêt de l'automatisation** : Effectuer des recherches manuelles sur Pastebin peut s'avérer extrêmement complexe si l'on utilise uniquement des requêtes classiques sur des moteurs de recherche. L'automatisation permet de surveiller en continu et à grande échelle les dépôts de texte afin d'y détecter rapidement des fuites d'informations critiques (telles que des listes d'identifiants, des mots de passe d'employés ou des données d'entreprise divulguées).

Comment mxtoolbox protège-t-il l'enquêteur ?

L'outil **MX Toolbox** protège l'enquêteur en agissant comme un **proxy** pour tester à sa place la connexion SMTP (sur le port TCP 25) d'un serveur suspect.

Cette méthode d'interrogation indirecte protège l'enquêteur contre trois risques majeurs qu'entraînerait une tentative de connexion directe depuis sa propre machine :

- **La journalisation de son identité** : Une connexion en direct permettrait au serveur distant d'enregistrer l'adresse IP publique de l'enquêteur dans ses fichiers journaux, compromettant ainsi la discrétion et l'anonymat de l'investigation.
- **Le risque de contre-attaque** : Si le serveur distant est contrôlé par un pirate informatique, celui-ci peut être configuré pour lancer une attaque informatique contre l'ordinateur de l'enquêteur dès qu'une tentative de connexion directe est détectée.
- **Les serveurs pièges (Honeypots)** : Le serveur ciblé peut s'avérer être un leurre piégé conçu spécifiquement pour repérer et ficher les professionnels de la sécurité et les enquêteurs qui tentent de l'analyser.

En déléguant la requête à MX Toolbox, l'enquêteur obtient les résultats de connectivité du serveur suspect sans jamais s'y exposer directement.

Quelle est l'utilité du site KnowEm ?

Le site **KnowEm** est un outil particulièrement utile pour les enquêteurs en raison de sa spécialisation dans l'analyse des pseudonymes en ligne. Ses principales fonctionnalités et utilités incluent :

- **La recherche multi-plateforme de pseudonymes** : KnowEm permet de vérifier si un nom d'utilisateur spécifique a déjà été enregistré ou utilisé sur **plus de 500 sites et réseaux sociaux différents**.
- **L'exploitation des routines des utilisateurs** : Les individus étant des êtres d'habitudes, lorsqu'une personne crée un pseudonyme (comme un pseudonyme sur Instagram), elle a de fortes chances de réutiliser exactement le même identifiant sur Facebook et de

nombreuses autres plateformes. KnowEm permet ainsi de cartographier l'ensemble des comptes publics associés à une même identité numérique pour y récolter des indices.

- **Une spécialisation sur les profils publics** : Contrairement à un outil comme Pipl qui croise des données diverses (adresses courriel, géolocalisation, etc.), KnowEm est **exclusivement dédié aux noms d'utilisateur des profils publics** sur les réseaux sociaux. Bien qu'il s'agisse à l'origine d'un outil de gestion de marque et de médias, les enquêteurs détournent ses fonctionnalités pour la recherche d'antécédents.

Conseil de sécurité : Les sources recommandent de bien cibler et de limiter vos objectifs de recherche avant d'utiliser cet outil, car il est extrêmement facile de se perdre dans la quantité de données et de résultats qu'il génère.

Qu'est-ce qu'une fuite d'IP ?

Dans vos sources, le terme « **fuites d'adresses IP** » est mentionné comme l'une des données techniques que les enquêteurs professionnels collectent et croisent avec les informations des réseaux sociaux, les données DNS et l'analyse forensique mobile pour identifier un individu. Bien que le document ne fournisse pas de définition théorique générale de ce qu'est une « fuite d'IP », il décrit très précisément plusieurs situations concrètes où l'exposition ou le masquage d'une adresse IP joue un rôle déterminant dans une enquête :

1. La fuite de l'adresse IP réelle à travers les en-têtes de courriels
Chaque fois qu'un courriel est acheminé, les serveurs de messagerie successifs inscrivent leur passage dans les lignes d'en-tête « Received », en y indiquant le nom du serveur et son **adresse IP**.

- **Preuve d'innocence** : C'est précisément l'analyse de ces adresses IP qui permet de confondre un usurpateur. Dans le cas de l'employé accusé de harcèlement, l'enquêteur s'attendait à trouver uniquement des adresses IP de serveurs internes. La présence d'adresses IP externes associées à un service de messagerie web et à un **VPN** a

révéle que le véritable expéditeur se situait à l'extérieur de l'entreprise, innocentant ainsi l'employé.

2. Le risque de fuite de l'IP de l'enquêteur

Lorsqu'un enquêteur tente de vérifier si un serveur suspect est actif en testant son port SMTP 25, il doit à tout prix éviter d'interroger directement l'adresse IP suspecte depuis sa propre machine.

- **Le danger** : Une connexion directe (via Telnet, par exemple) provoquerait une fuite de l'adresse IP de l'enquêteur, qui se retrouverait **enregistrée dans les fichiers journaux (logs) du serveur distant**. Cela détruirait l'anonymat de l'enquête et exposerait la machine de l'enquêteur à une contre-attaque si le serveur ciblé est contrôlé par un pirate ou configuré comme un piège (*honeypot*).
- **La parade** : L'enquêteur utilise un service tiers comme proxy (tel que MX Toolbox) pour effectuer le test de connexion sans dévoiler sa propre adresse IP.

3. Le masquage volontaire de l'IP par les attaquants

À l'inverse, les spammeurs et attaquants ont conscience que leur adresse IP peut les trahir. Lorsqu'ils utilisent des commandes manuelles via Telnet pour se connecter à des relais SMTP ouverts, ils transitent généralement par des **clients TOR ou des réseaux privés virtuels (VPN)** pour empêcher la fuite de leur véritable adresse IP d'origine et ainsi dissimuler leur identité et leur localisation géographique réelle.

Comment faire pour supprimer mes données de Zabasearch ?

Si vous découvrez vos informations personnelles sur un site de recherche de personnes comme **Zabasearch**, vous pouvez **vous opposer à la collecte et à l'affichage de vos données** (une procédure d'opposition ou d'opt-out) directement sur leur plateforme.

Cependant, les sources soulignent que cette démarche comporte d'importantes limites techniques et administratives :

- **Un délai de traitement long** : La procédure peut s'avérer vaine et frustrante. Le traitement de votre demande prend du temps, et vos informations personnelles peuvent **rester visibles pendant**

plusieurs mois après que vous avez soumis votre demande de suppression.

- **Un risque élevé de réapparition** : Vos informations peuvent **réapparaître subitement**. Dès que vous effectuez de nouvelles activités en ligne générant de nouvelles données, celles-ci sont automatiquement collectées, ce qui entraîne un nouvel affichage de votre profil sur ces plateformes.
- **La non-suppression des sources originales** : S'opposer à l'affichage sur Zabasearch bloque la visibilité de vos données uniquement sur ce site spécifique et pendant une certaine période. Cette action **ne supprime pas les documents administratifs originaux à la source** (registres d'État, dossiers judiciaires, actes de mariage, etc.), ni vos informations qui demeurent stockées et accessibles sur des dizaines d'autres sites similaires.

Comment fonctionne SimpleEmailSpoofers ?

SimpleEmailSpoofers est décrit dans vos sources comme un **projet open source** conçu pour **envoyer facilement des courriels falsifiés**.

Il s'agit d'un outil principalement utilisé par deux types de profils :

- Les **chercheurs** (pour analyser les vulnérabilités ou sensibiliser aux risques de sécurité).
- Les **spammeurs** (pour mener des campagnes d'usurpation d'identité).

Ce que les sources ne détaillent pas : Vos sources ne fournissent pas les détails techniques internes du fonctionnement de ce logiciel spécifique. Cependant, elles l'associent directement à d'autres méthodes d'usurpation d'identité par courriel, telles que :

- L'utilisation de serveurs d'envoi de courriels en masse.
- La connexion manuelle via Telnet (port 25) à un relais SMTP ouvert afin d'y saisir directement des commandes SMTP de base comme MAIL FROM: (pour falsifier l'adresse de l'expéditeur) et RCPT TO: (pour désigner le destinataire de l'attaque).

Comment l'OSINT démasque les fraudeurs ?

L'investigation de sources ouvertes (OSINT) permet de démasquer les fraudeurs en exploitant deux facteurs majeurs : le fait que **les individus sont des êtres d'habitudes** et l'existence d'une **empreinte numérique** publique que les suspects ne contrôlent pas entièrement.

Voici les principales méthodes décrites dans vos sources pour confondre les fraudeurs :

1. Détecter l'usurpation d'identité par recherche d'image inversée

Les escrocs et les agresseurs utilisent fréquemment de fausses photos de profil pour inspirer confiance en ligne. L'OSINT permet de contrer cela en effectuant une recherche inversée sur **Google Images** :

- En téléchargeant la photo suspecte, l'enquêteur peut voir l'ensemble des pages web où elle a été publiée.
- Si l'image remonte associée à **plusieurs noms, lieux ou professions différents**, l'enquêteur obtient la preuve que la photo a été volée ou usurpée.

2. Contourner la discrétion d'un suspect via son réseau professionnel

Un fraudeur peut se montrer très prudent, s'abstenir de publier la moindre photo de lui-même ou refuser d'être directement identifié sur les réseaux sociaux afin de dissimuler son activité. Les enquêteurs contournent ce silence en analysant son entourage professionnel :

- En utilisant des requêtes ciblant l'employeur du suspect, l'enquêteur peut faire remonter toutes les publications publiques de ses collègues de travail.
- **Exemple concret** : Dans un dossier d'assurance, un individu affirmait être paralysé à la suite d'un accident. Bien qu'il n'ait publié aucune photo de lui, une recherche axée sur son employeur a permis de découvrir des vidéos publiées par un de ses collègues de bureau, le montrant en train de **jouer un match de basket lors d'un barbecue d'entreprise**.

3. Exploiter les habitudes de géolocalisation pour localiser un suspect

Puisque les individus modifient rarement leurs habitudes de déplacement, l'analyse des enregistrements de présence publics (les *check-ins*) permet de cartographier précisément leurs routines :

- En formulant une requête pour lister les lieux visités par un profil (la requête places-visited), l'enquêteur identifie les endroits qu'un suspect fréquente de manière récurrente.
- **Exemple concret** : Cette technique a permis d'aider les autorités à arrêter un criminel en cavale en révélant qu'il se rendait dans **le même bar un mardi sur deux depuis deux ans**. Les forces de l'ordre ont pu l'appréhender en l'attendant simplement sur place le jour dit.

4. Relier des activités suspectes à travers des pseudonymes uniques
Par habitude, un utilisateur a tendance à **réutiliser le même nom d'utilisateur** sur différents réseaux sociaux, forums ou sites marchands. Des outils de corrélation de pseudonymes comme **KnowEm** ou **Pipl** permettent de croiser ces identifiants :

- L'enquêteur peut ainsi relier un profil de réseau social anonyme à un compte marchand (comme **eBay**).
- Cette méthode s'avère particulièrement utile en entreprise pour identifier un employé malveillant qui tenterait de **revendre du matériel informatique déclassé ou volé** (téléphones ou disques durs pouvant contenir des données confidentielles) sous un pseudonyme.

Peut-on identifier un pirate via Tor ou un VPN ?

L'identification directe d'un pirate utilisant **Tor** ou un **VPN** présente des défis techniques majeurs, mais les enquêteurs disposent de méthodes de recoupement pour remonter jusqu'à l'auteur d'un méfait :

- **Le but de l'utilisation de Tor ou d'un VPN** : Les attaquants se connectent généralement à des serveurs (comme des relais SMTP ouverts via le port 25) en utilisant un client Tor ou un VPN précisément pour masquer leur identité et empêcher la fuite de leur véritable adresse IP d'origine.

- **La détection de l'utilisation d'un VPN :** Bien que le VPN masque l'IP réelle de l'utilisateur, sa présence peut être détectée par l'enquêteur. Lors de l'analyse forensique des en-têtes d'un courriel, la découverte de lignes de réception (« Received ») provenant d'un service VPN indique clairement que le courriel provient de l'extérieur de l'entreprise (ce qui a permis, par exemple, de prouver l'innocence d'un employé faussement accusé).
- **L'identification par corrélation de données :** Pour identifier une personne qui dissimule ses traces derrière Tor ou un VPN, les enquêteurs professionnels ne se fient pas uniquement à l'adresse IP. Ils procèdent à une **corrélation d'informations multi-sources** en croisant de nombreuses technologies :
 - Les renseignements collectés sur les réseaux sociaux et l'étude des habitudes de la personne.
 - Les données DNS.
 - Les fuites d'adresses IP.
 - Les techniques d'analyse forensique des téléphones portables.
 - Les routines comportementales, telles que la réutilisation systématique d'un même pseudonyme sur différentes plateformes en ligne (détectable avec des outils comme KnowEm ou Pipl).

Ainsi, même si l'adresse IP d'origine est masquée à un instant T par un VPN ou Tor, c'est l'analyse globale de l'**empreinte numérique** laissée par le suspect à travers ses routines, ses publications et ses interactions qui permet finalement de l'identifier.

Peut-on identifier un fraudeur par sa photo ?

Oui, il est tout à fait possible d'identifier un fraudeur ou de révéler sa véritable identité en analysant sa photo grâce aux techniques d'investigation d'images présentées dans votre document :

1. **La recherche d'image inversée (Google Images) :**

- a. Les fraudeurs et les agresseurs mentent fréquemment en publiant des photos de profil qui ne sont pas les leurs afin d'inspirer confiance.
 - b. Pour vérifier l'authenticité d'une photo, un enquêteur peut la téléverser directement sur <http://googleimages.com>.
 - c. L'outil affiche alors tous les endroits du Web où cette image a été utilisée. Si la même photo apparaît associée à **plusieurs noms, localisations ou professions différents**, cela démontre que la photo a été volée ou usurpée.
2. **Le contournement par les photos d'identification (tags) sur Facebook :**
- a. Si un fraudeur prend soin de ne pas afficher son propre visage sur sa photo de profil public, l'enquêteur peut chercher à obtenir son **identifiant de profil Facebook unique (ID de profil)**.
 - b. En insérant cet identifiant dans une requête de recherche ciblée (le format d'URL photos-of), l'enquêteur peut afficher l'intégralité des images publiques **sur lesquelles d'autres personnes ont identifié (tagué) le suspect**. Cela permet de découvrir le véritable visage de la cible même si elle tente de rester anonyme sur son propre compte.

Comment fonctionne la recherche d'image inversée ?

La recherche d'image inversée (notamment à l'aide d'outils grand public comme **Google Images**) est une méthode simple et efficace pour vérifier l'authenticité d'un profil ou d'une preuve visuelle.

Voici comment elle fonctionne concrètement pour un enquêteur :

1. **Le téléversement de la photo suspecte** : L'enquêteur se rend sur <http://googleimages.com> et clique sur l'icône représentant un appareil photo afin de téléverser l'image qu'il souhaite analyser.
2. **La recherche de correspondance sur le Web** : Le moteur de recherche analyse l'image et affiche la liste de toutes les pages internet où cette même photo a été publiée ou utilisée.
3. **L'analyse des résultats pour déceler l'usurpation** :

- a. L'enquêteur cherche à valider si la photo est toujours associée à la même identité.
- b. Si les résultats de recherche révèlent que la même photo est liée à **plusieurs noms, professions ou localisations géographiques différents**, cela démontre de manière quasi certaine que l'image est fausse ou qu'elle a été volée pour créer un faux profil.
- c. Si l'image n'apparaît que sous un seul nom (ou des comptes de proches l'ayant identifié), cela tend à confirmer la véritable identité de la personne.

En plus de démasquer les utilisateurs de pseudonymes ou de fausses identités, cette méthode permet également aux analystes de résoudre rapidement des énigmes ou des défis visuels complexes en retrouvant instantanément les discussions et solutions associées à une image déjà publiée en ligne.