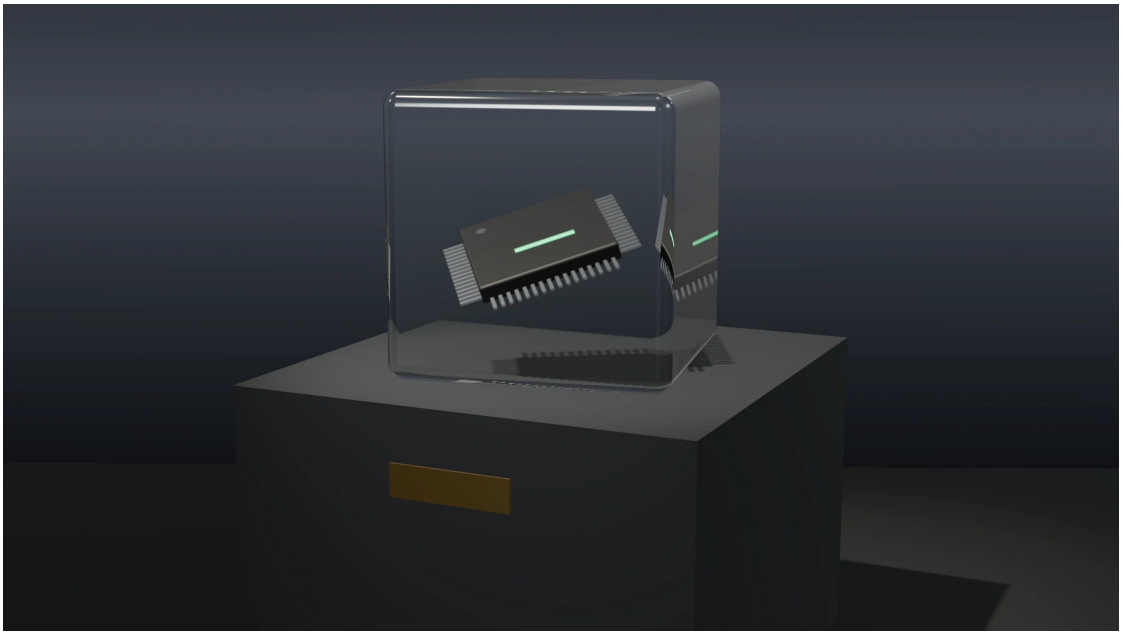
CONTACT

Expertiser un ordinateur saisi et répondre aux enquêteurs

Un ordinateur saisi dans une procédure pénale internationale : treize sources analysées et une réponse point par point aux questions d'un cabinet d'enquête londonien.

Version du 26 novembre 2026 — Imprimé le 26 novembre 2026



Le contexte

Un avocat de Suisse romande nous confie l'analyse d'un ordinateur portable saisi par la police dans une procédure pénale à dimension internationale. Nous recevons une copie de son disque, faite par les autorités, et nous travaillons exclusivement sur cette copie, en lecture seule.

Une première analyse porte sur les documents, la messagerie, l'historique de navigation et les comptes utilisés sur la machine. Le rapport est remis, la copie est restituée et nos données de travail sont détruites, comme le prévoit le mandat. Le dossier reviendra ensuite à plusieurs reprises.

Les questions d'un cabinet d'enquête londonien

Un cabinet d'enquête londonien, qui travaille sur l'affaire, avance que cet ordinateur aurait servi à se connecter au serveur d'une organisation. Ses enquêteurs nous posent leurs questions, par l'intermédiaire de notre mandant. Le procureur presse, il faut répondre vite et précisément: cet appareil est-il bien celui qui apparaît dans les journaux de connexion?

Pour y répondre, il faut l'adresse matérielle de sa carte réseau. Or l'outil d'analyse utilisé la première fois ne l'extrait pas. La copie du disque est retrouvée chez l'avocat, sur un support externe, et nous rouvrons le dossier.



Les questions posées

Les enquêteurs ne demandent pas «qu'y a-t-il sur ce disque?», mais des points précis, chacun capable de relier ou non l'ordinateur aux connexions observées:

- l'identifiant que l'annuaire Microsoft d'une organisation attribue à un appareil lorsqu'il s'y inscrit;
- l'adresse matérielle de chaque carte réseau, actuelle et passée;
- le nom de la machine, et ses éventuels changements;
- l'historique des réseaux Wi-Fi auxquels elle s'est connectée;
- l'usage d'adresses aléatoires, qui permet à un appareil de masquer sa véritable adresse sur un réseau.

Les outils

La première analyse a été menée avec Autopsy, un outil d'investigation libre: fichiers, messagerie, navigation, comptes, périphériques USB et Bluetooth, formulaires remplis, téléchargements. Il ne restitue pas les cartes réseau, d'où la reprise.

Pour celle-ci, l'image du disque, au format EnCase en dix-sept segments, est montée en lecture seule avec Arsenal Image Mounter. Les bases de registre sont lues avec Registry Explorer d'Eric Zimmerman, outil de référence du métier, puis interrogées par script (python-registry, python-evtx) pour que chaque valeur puisse être retrouvée et vérifiée par un tiers.

La profondeur de la recherche

Nous ne nous arrêtons pas au premier endroit où Windows range une information. Treize sources sont examinées, chacune avec son emplacement exact dans l'image:

- les ruches SYSTEM et SOFTWARE, qui décrivent le matériel, les cartes réseau et l'inscription aux annuaires;
- le profil de l'utilisateur (NTUSER.DAT), qui garde la trace des comptes d'organisation liés à la machine;
- les profils Wi-Fi enregistrés;
- les fichiers laissés par l'installation de Windows;
- quatre journaux d'événements: système, installation, ouverture de session et sécurité.

Les croisements

Une valeur isolée prouve peu. Nous croisons donc les sources entre elles: le même nom de machine, la même carte réseau et le même réglage des adresses aléatoires doivent se retrouver d'une source à l'autre, sinon il faut expliquer pourquoi.

Nous croisons ensuite ce que contient l'ordinateur avec ce que le cabinet londonien a relevé côté serveur. Le préfixe d'une adresse matérielle désigne le fabricant de la carte. Celui de l'ordinateur saisi ne correspond pas à celui des deux appareils vus dans les journaux de connexion. Enfin, l'identifiant d'appareil recherché est cherché aussi dans la ruche SOFTWARE, que le rapport du cabinet indiquait ne pas avoir consultée.

Trois détails techniques

- **Les cartes réseau** se lisent dans la ruche SYSTEM, sous ControlSet001\Control\Class\{4D36E972-E325-11CE-BFC1-080 une sous-clé par adaptateur installé, avec son pilote, son modèle et, le cas échéant, l'adresse imposée par l'utilisateur.
- **L'inscription à l'annuaire d'une organisation** laisse une trace dans le profil de l'utilisateur, sous les entrées WorkplaceJoin de NTUSER.DAT. Nous y avons trouvé deux comptes d'organisation, avec le nom d'appareil déclaré, mais pas l'identifiant recherché.
- **Les trois premiers octets d'une adresse MAC** (l'OUI) sont attribués par l'IEEE à un fabricant. Celui de l'ordinateur saisi désigne une puce Wi-Fi grand public. Ceux des deux appareils vus sur le serveur renvoient à des cartes montées dans la gamme professionnelle du même constructeur d'ordinateurs.

Ce que l'analyse établit

Aucun des identifiants recherchés n'apparaît dans les treize sources examinées. L'ordinateur n'a qu'une seule carte réseau, et les adresses aléatoires sont désactivées dans toutes les sources: aucune autre adresse sous laquelle il aurait pu se présenter n'apparaît. La différence de fabricant de carte avec les appareils vus sur le serveur n'avait pas été relevée dans le rapport du cabinet.

Nous écrivons ce que les traces permettent d'affirmer, et rien de plus: «n'apparaît dans aucune source examinée» n'est pas «ne s'est jamais connecté».

Les livrables

- Un rapport complet en deux parties: la démarche et les constats, avec la source de chaque constat.
- Une réponse condensée en anglais pour le cabinet londonien.
- Une lecture en langage simple du rapport du cabinet, pour l'avocat et le procureur, avec un encadré par notion technique.

Les noms, les identifiants et le contenu du dossier restent hors de cette page. Nous en présentons la démarche, jamais les pièces.

Investigation numérique · Toutes les réalisations