Techniques d'enquêtes

Les investigations numériques

Frédéric BATTAIS

LA PERQUISITION INFORMATIQUE

Elle consiste en rechercher, lire et examiner des données informatiques.

Deux notions importantes :
- rechercher des données,
- examiner des données.

On doit avant tout rester un enquêteur durant les opérations de visites et, lorsque cela est possible, garder à l'esprit la pertinence des saisies (entre les éléments probants les plus stratégiques et les données accessoires).

Pourquoi sommes nous aujourd'hui en visite domiciliaire dans les locaux de cette entité ?

Parce que (en France) le Juge des Libertés et de la Détention a désigné des agents habilités pour chercher et ramener des preuves de la fraude (fiscale) décrite dans l'ordonnance.

Ces preuves seront ensuite utilisées dans le cadre d'une autre procédure fiscale indépendante: la vérification de comptabilité.

Elles ne seront pas utilisées dans une procédure judiciaire comme dans le cas de l'informatique légale.

Il faut donc par tous les moyens à la disposition des enquêteurs qu 'ils cherchent et trouvent les preuves.

Qu'ils ramènent ces preuves de manière fiable, pour qu'elles puissent être opposées sans contestation de leur origine et de leur intégrité, dans une autre procédure fiscale.

Il faut donc que chacune de leurs actions, par une méthode rigoureuse et claire, garanties par la présence constante du représentant et de l'OPJ (Officier de Police Judiciaire), ne puissent mettre en cause l'authenticité et l'intégrité des preuves.

Il faut donc faire légalement des investigations informatiques.

L’investigation informatique doit respecter deux principes fondamentaux:

-L’intangibilité des données informatiques saisies: l’action d’investigation ne devra pas avoir pour effet de porter atteinte ou modifier l’intégrité des données informatiques.

-L’authenticité des données saisies: pour pouvoir servir de preuves, les données informatiques devront être authentifiées et figées dans le temps.

L’utilisation d’un logiciel d’investigation numérique (forensique) assure le blocage en écriture des supports investigués.
L’examinateur ne peut modifier le contenu des fichiers.

Le blocage en écriture peut être:

- logique dans ce cas il est effectué par le logiciel,
- physique par la connexion du support investigué à un bloqueur physique (type Tableau).

(En France c'est) L'article L 16B du Livre des Procédures Fiscales

- **Périmètre d'investigation :**

- Le JLD autorise « les agents de l'administration des impôts, ayant au moins le grade d'inspecteur et habilités à cet effet par le directeur général des finances publiques, à **rechercher la preuve de ces agissements**, en effectuant des visites en tous lieux, même privés, où les pièces et documents s'y rapportant sont susceptibles **d'être détenus ou d'être accessibles ou disponibles et procéder à leur saisie, quel qu'en soit le support**. »

- **Obligations juridiques :**

- Un procès-verbal relatant les modalités et le déroulement de l'opération et consignant les constatations effectuées est dressé sur-le-champ par les agents de l'administration des impôts. **Un inventaire des pièces et documents saisis lui est annexés s'il y a lieu**. Le procès-verbal et l'inventaire sont signés par les agents de l'administration des impôts et par l'officier de police judiciaire ainsi que par les personnes mentionnées au premier alinéa du III ;
- Les pièces et documents saisis sont **restitués** à l'occupant des locaux dans les six mois de la visite ; toutefois, lorsque des poursuites pénales sont engagées, leur restitution est autorisée par l'autorité judiciaire compétente.

SE PRÉPARER AVANT L'INTERVENTION

Inventaire matériel

Préparation des supports de saisies

(prévoir plusieurs types de support clé usb ou disques durs de capacité différente)

Formater ou wiper les supports déjà utilisés pour enlever toutes traces de fichiers antérieurs, sans objet avec l'intervention.

Réunion préparatoire: organisation informatique connue ?

Nombre de postes à investiguer ?

Nature de la fraude présumée (=> type de fichiers à saisir).

QUE CHERCHER (une démarche)

Que cherche-t-on à démontrer ?
Cela va dépendre de la nature de l'affaire, carrousel TVA, établissement stable (SDE), …

Quels éléments seraient susceptibles d'étayer les présomptions de fraude ?
Des documents comptables ? Commerciaux ? Application « Métier » ?
Des échanges de mails ou de messagerie instantanée ? En anglais ?
Garder à l'esprit la pertinence des documents recherchés/trouvés si ils sont ensuite transmis à unservice vérificateur.
(ce qui doit guider la sélection des fichiers saisis)

Qui pourrait émettre ou détenir ces documents ?
Un dirigeant ? Un responsable de service ? Un personnel de support ? Du personnel ayant quitté ses fonctions ?

Où peuvent se situer ces documents ?
Suivant l'ancienneté des faits, sont-ils encore en ligne ? Archivés ? Dans une boite mail ? A l'étranger ? Sur un serveur distant ? Dans le cloud ? Sur un support externe ? Dans une application « métier » ?

QUE CHERCHER (une démarche)

Comment y accéder (à ces données)?
Problématiques d'accès à des serveurs distants (droits d'accès), d'accès à des partitions cryptées, à des espaces d'archives, problème de droits d'exécution, …
C'est la partie « technique informatique ». Ce questionnement doit venir aiguiller la présentation du SI que l'on demande en début d'opération.

pour mémoire, voici une organisation type de SI :
- un espace serveur distant personnel (et répliqué/sauvegardé automatiquement !) de Z à I suivant le mapping mis en place par la société
- un espace similaire pour le service concerné (H ou autre volume)
- un espace d'échange de fichiers
- dont un éventuel répertoire de modèles type de documents
- une ou des applications « métier » (en plus de la comptabilité si pas en ERP)
- une messagerie professionnelle, une messagerie personnelle
- une partie « Drive » ou « Cloud »

Ces préconisations mises en place par les sociétés sont plus ou moins suivies par les employés. L'espace disque local demeure toujours intéressant à investiguer !

Déroulement d'une intervention : Entrée dans les locaux

Détermination d'une méthode d'investigation.
Elle dépend de:

1) Organisation informatique de l'entreprise :

- Nature du réseau et du mode de stockage de données (sur serveur, sur pc individuel; serveur dans les locaux ou distant)

-Présence de l'administrateur réseau,

-Droit d'accès au serveur,

-Cryptage des données,

-Les ports USB des ordinateurs sont-ils activés pour l'exportation des données ?

-Type de messageries utilisées :
sur poste visité en local, sur un serveur de messagerie (localisation, accès), Webmails,..
- Les fonctions de copie ou d'export sont-elles disponibles ?

Déroulement d'une intervention : Entrée dans les locaux

2) Ciblage des postes informatiques à investiguer (prioritaires puis secondaires)

Localisation de l'équipe des Officiers de Police Judiciaire

Présence de l'utilisateur (afin de pouvoir gérer un départ éventuel)
Accès au poste informatique
Gestion des mots de passe utilisateur

Accès direct aux données sur le serveur

Souvent on est en présence d'un nombre supérieur de postes à investiguer que de dotations d'investigations informatiques présentent sur le point.

Première étape

Estimer rapidement l'organisation mise en place par l'utilisateur (fichiers organisés ou en vrac, état du bureau, etc ...)

Voir les fichiers présent dans la corbeille

Regarder les documents récents

Regarder les historiques et favoris internet

Procéder à la visualisation de l'intégralité du disque

Regarder les programmes installés (Démarrer, Programmes)

Repérer les logiciels de rapatriement de mail (Outlook, Gmail, Windows mails etc...)

Vérifier si les fichiers mails sont stockés en local sur le disque (ou si distants/webmails)

Recherche et sélection des fichiers en rapport avec la fraude

Étude de l'arborescence

La visualisation des fichiers récents sur lesquels l'utilisateur du PC a travaillé permet de localiser la zone sur le disque dur ou sur le serveur de l'entreprise sur laquelle il travaille habituellement.

Lorsque la fraude recherchée est fiscale et non pénale, les utilisateurs ne cherchent pas systématiquement à cacher les fichiers.

Généralement une étude de l'arborescence de la zone de travail, ou de celle de l'ordinateur, permet de trouver des fichiers liés à la fraude.

Recherche par « mots clés »

Ce mode de recherche paraît plus simple mais avec des résultats beaucoup plus aléatoires:

Dépend du mode d'indexation du moteur de recherche de l'orthographe du mot, de la casse, du lieu ou l'on a situé la recherche.

Nature de fichiers recherchés

Les fichiers à rechercher sont définis au cours de la réunion préparatoire à l'intervention.

Ils dépendent de la nature de la fraude et donc du faisceau d'indices que l'on cherche à rassembler pour la prouver.

Cela peut être par exemple des fichiers PDF car ils peuvent correspondre à des contrats signés. Mais on pourra aussi rechercher les fichiers WORD relatifs à la constitution de ces contrats car il indique sur quel ordinateur il a été créé (clic droit onglet propriété, cette information fait partie des métadonnées).

Masque de factures

ETC…….

Cas des messageries

Aujourd'hui les messageries, qu'elles soient professionnelles ou personnelles, ont pris une place prépondérante dans les saisies à effectuer.

Une part très importante des données d'une société transite via les pièces jointes attachées aux messages.

Quels types de messageries connaissez-vous ?

Il existe deux grands types différents de messageries :

- Les messageries locales, de type Outlook.
Elles représentent encore bien plus de la moitié des boites mails rencontrées.

- Les messageries distantes Webmail (type Gmail).

Il est à noter que maintenant même les messageries ‘locales’ comme Outlook migrent vers des modèles de plus en plus distants (Outlook 365). Se pose donc aussi pour elles le problème de l’accès et du rapatriement.

Méthodes de saisie

Il existe différentes méthodes de saisie possibles. Elles sont cumulables entre elles.
(Ainsi, si on a peu de messages intéressants on peut juste les imprimer).

Pour les messageries de type Outlook
- Impression
- Glisser-déposer
- Etiquettes
- Création d'un fichier de données : saisie sélective
- Création d'un dossier
- Saisie globale (clone) / Création d'un fichier de données 'avocats' et on saisit la messagerie vivante

Pour les messageries Webmail, il faudra rapatrier les données en local avant de les saisir.

Le rapatriement en local peut être fait utilisant en utilisant les fonctions du Webmail (Google takeout).

On peut également utiliser un logiciel spécifique (comme Thunderbird portable). Cette solution est plus compliquée à mettre en œuvre.

Le rapatriement de ces données sur le poste visité se fait:
dans un répertoire spécifique,
créé par l'agent investigateur,
pour les différencier des données locales.

Autres systèmes

Bien entendu, dans la mesure du possible, et en fonction des différents cadres juridiques en vigueur, il conviendra aussi de s'intéresser possibilités d'investigation sur les réseaux sociaux.

Les principaux sont:
- Facebook
- Instagram
- Snapchat
- WhatsApp

...

A retenir

Comme pour les messageries, ces applications proposent généralement à leurs utilisateurs des fonctionnalités d'exportation de données. C'est là-dessus que l'on peut s'appuyer.

Problématique du secret de la correspondance entre un avocat et son client

Il s'agit, pour se conformer à la législation en vigueur (en tout cas en France), d'extourner les mails d'avocats des saisies dans les messageries.

Qu'elles soient locales ou distantes, les mails présents dans les messageries doivent faire l'objet d'un tri aux fins d'extourner les mails « de » et « à » des avocats (dont la liste est fournie en cours d'intervention).

Si la messagerie est distante:
Soit on travaille sur la messagerie rapatriée, (l'originale étant restée sur le serveur distant, l'utilisateur conserve la totalité de ses mails, protocole IMAP).
Soit (cas le plus fréquent) on n'a rapatrié que les mails en rapport avec la fraude décrite en créant un libellé spécifique. (le takeout.zip est rapatrié en étant filtré)

Autres cas de secrets professionnels ? (médical, ...)

Données stockées sur un serveur local ou distant

Soit on y a accès à partir d'un des postes informatiques investigués

(cela peut passer par l'obtention des codes d'accès administrateur pour avoir accès à toutes les données)

Rapatriement de ces données sur le poste visité dans un répertoire spécifique créé par l'agent investigateur pour les différencier des données locales.
Utiliser un nom de répertoire court, « serveur X : »
(Problématique de chemins longs, vigilance avec W 10)

Soit accès direct sur le serveur de données
(Là encore, s'assurer que l'on a bien obtenu les codes d'accès administrateur pour avoir accès à TOUTES les données)
Copie des données sur un disque dur externe (support de saisies)

Problématique des données cryptées

Si l'ordinateur est en utilisation et que les données cryptées sont accessibles (l'utilisateur ayant saisi son mot de passe), alors on pourra copier les données sur un support non crypté.
MAIS il faudra bien s'assurer que le copier/coller m'emmène pas le cryptage !

Si l'ordinateur est éteint ou que l'utilisateur refuse de saisir ses mots de passe de décryptage, il reste la possibilité de mise sous scellés du matériel considéré.
(comme aux échecs, la menace étant souvent plus forte que la mise la mise en pratique réelle)

Finalisation des opérations d'investigations

Ces opérations doivent être menées de manière très rigoureuse car elles conditionnent directement le succès ou l'échec d'une opération.

C'est elles qui sont garantes de l'intangibilité et de l'authenticité des données saisies.

Elles sont réalisées en fin d'intervention.

(En France) Le texte L 16 B prévoit que l'on doit dresser un inventaire des fichiers saisis et que ces derniers doivent être restitués dans un délai de 6 mois.
Il faut pouvoir prouver que les fichiers restitués sont strictement les même que ceux saisis.
D'autre part, ces fichiers sont destinés à être utilisés au cours d'une procédure d'examen de comptabilité, et être opposés à l''entreprise.
Pour que cette opposition soit probante il faut que le vérificateur puisse justifier de l'origine du fichier ainsi que de son intégrité.

Calcul d'une clé de Hash par fichier saisis

La clef de 'Hashage' est obtenue grâce à un algorithme.
Elle est la **signature numérique** du fichier.

Cette clé est calculée en fonction d'éléments propres à chaque fichier (données et métadonnées).
Toute modification des données fichier, modifie directement la clé de hash.
(il est à noter que ouvrir et fermer un .pst OUTLOOK modifie cette clef de Hash)

Cette clé va prouver que le fichier restitué, ainsi que celui opposé par le vérificateur, est bien le même que celui qui a été saisi dans la procédure. Cela garanti qu'il n'y a pas eu de modification de ce dernier.

Les logiciels forensiques calculent une clé de hash par fichier.
Les plus connus sont SHA 256 et SHA 512 (ne plus utiliser MD5).
(logiciel gratuit disponible sur internet : QuickHash)

Réalisation de l'inventaire

L'inventaire consiste en la liste des noms des fichiers saisis. Il faut indique dans ses inventaires le chemin des fichiers et pas seulement leur nom.

Les logiciels forensiques permettent d'indiquer le chemin d'origine du fichier saisis (lieu où il était enregistré sur le disque dur investigué).

En utilisant un logiciel forensique et en indiquant le nom et le chemin d'origine du fichier ainsi que sa clé de Hash au moment de la saisie, l'authenticité ainsi que l'intangibilité des données est préservée.

Cet inventaire peut être établi sous la forme d'une impression (si peu de pages) ou bien d'un fichier informatique.
Il faut vérifier qu'il correspond bien à la totalité des fichiers saisis.
L'inventaire est (en France) une annexe au PV de visite.

Rédaction du PV Informatique

La partie des investigations numériques doit venir s'insérer dans le Procès Verbal (PV) général. C'est en général les personnes qui ont procédé aux investigations qui la rédige.

Il conviendra donc durant les investigations de veiller à prendre quelques notes qui seront précieuses au moment de la rédaction.

Ainsi, on prendra soin de bien identifier chaque poste ou support (clé USB, disque dur externe, CD-DVD/ROM, …) de la manière la plus précise (marque, modèle, localisation, personne l'utilisant, fonction et localisation) et la plus unique possible. On décrira ensuite plus sommairement les saisies effectuées sur ces matériels (ou via ces matériels pour toute la partie distante réseau/cloud accessible depuis ce poste).

Quelques exemples possibles de rédaction du PV (à titre indicatif)

Cas général

L'ordinateur portable de marque HP, modèle Pro, présent dans le bureau de M. Jean Martin, directeur commercial de la société S

a. Fichiers/Documents

Nous avons constaté, sur ce matériel, la présence de fichiers entrant dans le champ de l'autorisation de visite et de saisie délivrée par le Juge des Libertés et de la Détention et avons sélectionné lesdits fichiers.

b. Adresse de messagerie : jean.martin@outlook.fr

Nous n'avons pas constaté au sein de cette messagerie la présence de documents entrant dans le champ de l'autorisation de visite et de saisie délivrée par le Juge des Libertés et de la Détention.

c. Disque dur externe de marque TOSHIBA d'une capacité de 2 To présent dans le bureau de M. T

Nous avons constaté, sur ce matériel, la présence de fichiers entrant dans le champ de l'autorisation de visite et de saisie délivrée par le Juge des Libertés et de la Détention et avons sélectionné lesdits fichiers.

d. Clé USB de marque SANDISK d'une capacité de 64Go présente dans le bureau de M. T

Nous n'avons pas constaté au sein de ce support la présence de documents entrant dans le champ de l'autorisation de visite et de saisie délivrée par le Juge des Libertés et de la Détention.

L'OCCUPANT consent à nous donner accès au serveur de données « \\... ».

A partir d'un ordinateur (marque, modèle) mis à notre disposition, nous avons examiné le contenu de la zone serveur et avons constaté la présence de documents...

L'ordinateur fixe de bureau de marque DELL, modèle P, présent dans le bureau de M. Paul Dupond, dirigeant de la société S

a. Fichiers/Documents

Nous n'avons pas constaté la présence de documents entrant dans le champ de l'autorisation de visite et de saisie délivrée par le Juge des Libertés et de la Détention.

b. Adresse de messagerie: paul.dupond@gmail.fr

L'examen depuis l'ordinateur mentionné ci-dessus de l'adresse de messagerie paul.dupond@gmail.fr a permis de constater la présence de documents entrant dans le champ de l'autorisation de visite et de saisie délivrée par le Juge des Libertés et de la Détention.
En utilisant les fonctionnalités d'un client de messagerie portable nous avons procédé au rapatriement des données de cette messagerie en local sur l'ordinateur référencé ci-dessus (dossier C:\Pt2_Paul_D).
Le fichier nommé paul.dupond@gmail.fr.zip a été sélectionné en vue de sa saisie ultérieure.

c. Espace de stockage Google Drive lié au compte de messagerie paul.dupond@gmail.fr

L'examen depuis l'ordinateur mentionné ci-dessus de l'espace de stockage en ligne Google Drive lié au compte de messagerie paul.dupond@gmail.fr a permis de constater la présence de documents entrant dans le champ de l'autorisation de visite et de saisie délivrée par le Juge des Libertés et de la Détention.
Il a été procédé au téléchargement, dans le dossier C:\Pt2_Paul_D, des documents en lien avec la fraude présumée présent dans cet espace à l'aide des options de téléchargement des données du compte Google.
Le fichier nommé takeout-20220303T211230Z-001.zip a été sélectionné en vue de sa copie ultérieure.

Les fichiers sélectionnés ont été copiés sur une clé USB vierge, neuve sous blister, appartenant à l'administration préalablement formatée en présence de M. Patrick T, représentant de la société S et de Mme D M, OPJ.
Nous avons procédé à l'authentification numérique de chaque fichier et avons élaboré un inventaire.

Les Investigations Informatiques

Au final, on vient pour rechercher, collecter, trier et saisir des éléments de preuve concernant une fraude présumée. (recueillir un faisceau d'indices)

Lors de la préparation de l'intervention, on aura déjà une idée la plus précise possible de ce que l'on cherche, sous quelle forme de fichier le trouver, qui est susceptible de détenir cette information, de la créer, de la recevoir, de la modifier…

On organisera les investigations sur place en fonction de l'organisation, des matériels et des personnes présents. On établira une priorisation des postes à investiguer.

Pour terminer, on établi un inventaire des fichiers saisis et on rédige le Procès-Verbal (PV).

QUESTIONS

Merci de votre attention

Et bon courage à vous dans vos opérations futures!