

Fundamentals of Digital Forensic Investigation Procedures

Ce texte présente un guide complet sur la **méthodologie des enquêtes médico-légales numériques**, en mettant l'accent sur les aspects techniques et procéduraux nécessaires pour mener un dossier à terme. L'auteur détaille les étapes cruciales de la **phase de pré-enquête**, incluant la formation du premier intervenant, la sécurisation de la scène de crime et l'obtention des autorisations légales. Une importance majeure est accordée à la **documentation rigoureuse** et à l'utilisation d'outils spécialisés comme Autopsy pour consigner chaque action sans compromettre l'intégrité des preuves. Le document insiste également sur le respect de l'**ordre de volatilité des données** et l'interdiction formelle de manipuler des éléments originaux. Enfin, il souligne que la **crédibilité des rapports d'expertise** dépend de la précision des notes prises tout au long du processus d'investigation.

Quelles sont les étapes clés d'une enquête médico-légale numérique ?

Une enquête médico-légale numérique suit un processus rigoureux qui va de la préparation initiale à la présentation des résultats. Selon les sources, les **étapes génériques** d'une telle enquête sont les suivantes :

- **Déterminer si un incident s'est produit.**
- **Identifier tous les indices** qui ont été laissés derrière soi.
- **Lancer une évaluation préliminaire** de la situation et identifier les preuves potentielles.
- **Rechercher et saisir des artefacts** contenant des preuves potentielles.
- **Recueillir des preuves** et les transmettre pour une utilisation légale potentielle.
- **Mettre fin à l'implication active.**
- **Rédiger un rapport d'enquête.**

Pour approfondir ces étapes, le processus peut être divisé en plusieurs phases clés :

1. Pré-enquête et Préparation

Avant de commencer, l'équipe doit comprendre l'objectif de l'enquête, le contexte de l'affaire (qui est impliqué, l'impact sur l'organisation) et s'assurer qu'elle dispose des **autorisations ou mandats nécessaires** pour accéder aux systèmes. Il est également essentiel d'évaluer l'effort requis en termes d'outils et de ressources humaines.

2. Intervention initiale et Ouverture du dossier

Le **premier intervenant** joue un rôle crucial en isolant la zone de l'incident et en documentant l'état actuel de tous les systèmes impliqués (vidéos, photos, horodatage) pour éviter toute contamination des preuves. L'ouverture d'un dossier implique la prise de notes systématique, idéalement via un **logiciel de gestion de cas** comme Autopsy, pour consigner la date, l'heure, le lieu et les personnes présentes.

3. Saisie et Collecte des preuves

La règle d'or est de **ne jamais examiner l'élément original** pour éviter de le modifier. Les enquêteurs doivent :

- Créer plusieurs **copies numériques** de l'élément.
- Valider ces copies par des **fonctions de hachage**.
- Collecter les données par **ordre de volatilité** (des registres/cache vers les supports d'archivage) pour ne pas perdre d'informations cruciales en cas de coupure de courant.
- Utiliser des **sacs de protection** (antistatiques ou cages de Faraday) pour le transport et maintenir une **chaîne de traçabilité** documentée.

4. Analyse et Constatations

Cette phase se concentre sur l'examen des copies des artefacts pour identifier des preuves sans compromettre leur validité légale.

L'enquêteur documente chaque action menée et chaque élément trouvé en précisant la méthode employée.

5. Rapport médico-légal et Clôture

Le rapport final est la partie la plus visible de l'enquête. Il doit être clair, objectif et inclure au minimum :

- Un **résumé de l'affaire**.
- Les détails de l'**acquisition et de la préparation** des preuves.

- Les **constatations** détaillées et la **conclusion** basée uniquement sur les faits.
- La liste des auteurs et leurs signatures.

Enfin, l'implication officielle dans le dossier prend fin (clôture), suivie d'une **analyse critique** pour évaluer la maturité des pratiques de l'équipe et identifier des pistes d'amélioration.

Quels logiciels de gestion de cas recommandez-vous ?

Les sources recommandent plusieurs logiciels de gestion de cas, allant d'options gratuites et accessibles aux solutions professionnelles robustes. L'utilisation de tels outils est jugée **cruciale** pour maintenir l'organisation d'une enquête qui peut rapidement devenir chaotique en raison de la quantité massive de données générées.

Voici les recommandations spécifiques extraites des sources :

1. Option gratuite et accessible : Autopsy

Le logiciel **Autopsy**, disponible gratuitement (notamment sous Kali Linux), est mis en avant comme une excellente solution pour débiter.

- **Fonctionnalités** : Bien qu'il serve principalement à l'analyse d'images disque, il permet de créer un dossier, d'y ajouter des périphériques (hôtes) et de documenter chaque étape via un **séquenceur d'événements** qui fait office de journal numérique.
- **Limites** : Les sources notent toutefois qu'il présente certaines lacunes pour l'exportation de données par rapport à des logiciels d'entreprise.

2. Options populaires pour un usage professionnel

Pour un cadre professionnel, les sources recommandent d'explorer des solutions plus performantes et offrent davantage d'options d'enregistrement :

- **Digital Forensic Framework (DFF)**
- **Open Computer Forensics Architecture (OCFA)**
- **X-Ways Forensics**
- **EnCase**

3. Outils complémentaires et alternatives

- **Microsoft Word ou OneNote** : À minima, si vous ne disposez pas d'un logiciel spécialisé, il est conseillé d'utiliser des modèles de formulaires préétablis sur ces outils.
- **TimeLive** : Ce logiciel est recommandé spécifiquement pour le **suivi des heures de travail et la facturation**, une fonctionnalité que des outils comme Autopsy ne proposent pas.
- **Draw.io** : Pour la création de schémas de réseau nécessaires à la documentation du dossier, cet outil gratuit basé sur le cloud est suggéré, tout comme **LucidChart** ou **Dia Diagram**.

Les sources vous conseillent de **tester plusieurs de ces options** afin de déterminer celle qui correspond le mieux à votre style d'enquête personnel. Chacun de ces logiciels sera probablement plus efficace que l'utilisation de simples notes papier pour gérer la complexité d'une investigation numérique.

Quels outils de schémas de réseau utiliser ?

Pour élaborer des schémas de réseau dans le cadre d'une enquête médico-légale, les sources mentionnent plusieurs options allant des logiciels professionnels aux solutions gratuites en ligne :

Outils professionnels et bureautiques

De nombreux enquêteurs utilisent des logiciels classiques de présentation ou de conception pour créer leurs schémas :

- **Microsoft Visio** : Très utilisé pour les schémas techniques.
- **Microsoft PowerPoint** : Une option plus généraliste pour la schématisation.
- **Produits Adobe** : Utilisés pour élaborer des schémas plus complexes ou visuels.

Solutions gratuites et basées sur le cloud

Si vous recherchez des outils plus accessibles ou ne nécessitant pas d'installation, les sources recommandent :

- **Draw.io** (proposé par SolarWinds) : C'est une solution gratuite, simple d'utilisation et basée sur le cloud qui ne nécessite aucune installation.
- **LucidChart** : Une alternative populaire basée sur le cloud.

- **Dia Diagram** : Une autre option mentionnée pour répondre aux besoins de schématisation.

L'utilisation de ces outils est particulièrement recommandée lorsque vous devez enquêter sur un réseau en production afin d'en comprendre le **périmètre**, le **flux de données** entre les systèmes, et d'identifier les périphériques présents sur chaque segment. Les sources conseillent de consigner ces schémas directement dans votre **logiciel de gestion de cas** pour maintenir l'organisation de vos constatations.

C'est quoi l'ordre de volatilité des données ?

L'**ordre de volatilité** est un principe fondamental de la criminalistique numérique qui stipule que les données doivent être collectées en commençant par les plus fragiles, c'est-à-dire celles qui risquent le plus d'être perdues ou modifiées si l'état de l'appareil change (comme lors d'une mise hors tension).

Selon les sources, qui s'appuient sur les recommandations de l'IETF (RFC 3227), les artefacts de données sont classés du **plus volatil au moins volatil** selon l'ordre suivant :

1. **Registres et Cache** : Le cache et les registres du processeur sont extrêmement volatils car ils changent en quelques nanosecondes.
2. **Tables et Mémoire vive (RAM)** : Cela inclut les tables de routage, le cache ARP, la table des processus et les statistiques du noyau. Ces données sont en constante évolution et sont **définitivement perdues** en cas de coupure de courant.
3. **Systèmes de fichiers temporaires** : Bien qu'ils puissent être perdus lors d'une extinction, ces fichiers ont tendance à persister davantage que les éléments précédents et sont parfois récupérables.
4. **Disque dur (HDD et SSD)** : Les données y sont conçues pour être sauvegardées, le risque de perte est donc faible. Toutefois, les disques SSD récents possèdent des algorithmes (comme TRIM) qui peuvent altérer les données de manière autonome.
5. **Données de journalisation et surveillance à distance** : Ces journaux sont généralement stockés, mais ils sont plus

susceptibles d'être perdus que les données d'un disque dur local et sont considérés comme ayant moins de valeur pour l'enquête.

6. **Configuration physique et topologie réseau** : Ce sont des éléments stables qui présentent généralement peu d'intérêt immédiat pour l'analyse.
7. **Supports d'archivage** : Il s'agit de supports anciens (bandes, sauvegardes externes) dont les données sont les moins précieuses car les plus datées.

Pourquoi cet ordre est-il crucial ?

Maintenir l'alimentation d'un appareil est essentiel pour capturer les données volatiles. Par exemple, de nombreux **logiciels malveillants** s'exécutent uniquement en mémoire vive et ne s'installent jamais sur le disque dur ; ils disparaîtraient donc totalement si l'on éteignait l'ordinateur avant la collecte. De plus, le simple fait de redémarrer un système modifie son "hachage" (sa signature numérique), ce qui peut être interprété comme une **contamination des preuves** dans un cadre juridique.

L'enquêteur peut toutefois adapter cet ordre selon les besoins spécifiques de l'affaire. Par exemple, si la RAM d'un système n'est pas jugée pertinente pour l'enquête, l'effort peut être redirigé prioritairement vers la copie du disque dur.

Quelle est la règle d'or pour manipuler l'original ?

La règle d'or (ou règle principale) en criminalistique numérique est de **ne jamais examiner l'élément original**.

Le respect de cette consigne est impératif pour les raisons suivantes :

- **Prévention de la contamination** : Toute modification apportée à l'original, même involontaire, risque d'être considérée comme une contamination.
- **Validité légale** : Une telle altération compromet l'utilisation légale des preuves devant les tribunaux, ce qui peut mener au classement sans suite d'une affaire.
- **Intégrité des données** : Le simple fait de redémarrer un système peut modifier sa signature numérique (hachage), ce qui est

interprété comme une altération de la preuve dans la plupart des contextes juridiques.

Au lieu de manipuler l'original, les sources préconisent de suivre systématiquement ces trois étapes sur tout élément numérique collecté :

1. **Créer plusieurs copies numériques** de l'élément.
2. **Valider le hachage** de ces copies pour garantir qu'elles sont identiques à l'original.
3. **Activer la protection en écriture** avant de procéder à l'examen de la copie.

Comment protéger un disque en écriture ?

La protection en écriture est une étape cruciale pour garantir l'intégrité des preuves numériques et éviter toute contamination qui pourrait invalider une enquête devant les tribunaux.

Selon les sources, il existe deux méthodes principales pour protéger un disque en écriture :

- **Les dispositifs matériels (bloqueurs d'écriture)** : Il s'agit de périphériques physiques spécialisés, comme le **Logicube-MD5**, ou de duplicateurs de disques portables intégrant une fonction de blocage en écriture. Ces outils s'interposent physiquement entre le disque suspect et l'ordinateur de l'enquêteur pour empêcher tout signal d'écriture d'atteindre le support original.
- **Les solutions logicielles** : Il est possible d'utiliser des **logiciels de blocage en écriture** installés directement sur l'ordinateur portable d'investigation.

Procédure recommandée : Dans la pratique, l'enquêteur doit activer cette protection **avant même de connecter le disque** ou d'examiner une copie numérique. Par exemple, une procédure standard consiste à activer le blocage en écriture sur la machine d'analyse, puis à se connecter au disque d'intérêt (par exemple via un câble USB) pour procéder à la création des copies numériques sécurisées.

Toutes les mesures de protection en écriture appliquées lors de l'enquête doivent être scrupuleusement consignées dans le **rapport d'expertise judiciaire** pour prouver qu'aucune altération n'a eu lieu.

Comment capturer les données de la RAM ?

La capture des données de la **mémoire vive (RAM)** est une étape critique car elles sont considérées comme **volatiles** : elles sont en constante évolution et sont **définitivement perdues** si l'appareil est mis hors tension.

Pour capturer ces données efficacement selon les sources, voici les principes à suivre :

- **Maintenir l'alimentation** : Il est impératif de ne pas éteindre ou redémarrer le système avant la capture, car cela détruirait les données volatiles et modifierait la signature numérique (hachage) du système, ce qui pourrait être considéré comme une contamination des preuves.
- **Respecter l'ordre de volatilité** : Selon les normes de l'IETF, la RAM figure en deuxième position sur l'échelle de volatilité (juste après les registres et le cache du processeur). Elle doit donc être collectée **prioritairement**, bien avant de procéder à la copie des disques durs.
- **Effectuer un « dump »** : La procédure consiste à extraire le contenu de la mémoire sous la forme d'un fichier image, par exemple un **dump RAM au format .raw**.
- **Organisation et documentation** : Une fois l'extraction réalisée, il est conseillé de placer ces éléments dans un **dossier spécifique** (par exemple, un sous-dossier « RAM ») au sein de votre logiciel de gestion de cas comme Autopsy afin de maintenir une organisation rigoureuse.
- **Outils spécialisés** : Bien que les sources mentionnent qu'Autopsy permet d'importer et d'analyser ces captures, elles précisent que les outils techniques spécifiques et les procédures d'extraction détaillées pour les terminaux font l'objet d'un développement approfondi dans le **chapitre 7** de l'ouvrage de référence.

La capture de la RAM est particulièrement précieuse pour identifier des **logiciels malveillants** qui s'exécutent uniquement en mémoire sans laisser de traces sur le disque dur, ou pour récupérer des processus en cours d'exécution au moment de l'incident.

Comment analyser le fichier .raw ?

L'analyse d'un fichier **.raw** (généralement un **dump RAM**) s'effectue principalement à l'aide de logiciels de gestion de cas et d'analyse forensique, les sources mettant particulièrement en avant l'utilisation d'**Autopsy**.

Voici la procédure pour analyser ce type de fichier selon les sources :

1. Préparation dans Autopsy

- **Ouvrir le logiciel** : Sous Kali Linux, Autopsy est accessible via une interface graphique à l'adresse <http://localhost:9999/autopsy>.
- **Créer ou ouvrir une affaire** : Vous devez d'abord configurer le cadre de l'enquête en saisissant le nom de l'affaire et les enquêteurs impliqués.
- **Ajouter un hôte** : Créez une entrée pour le périphérique dont provient le fichier .raw.

2. Importation du fichier .raw

Une fois l'hôte créé, vous devez importer le fichier en suivant ces étapes (illustrées dans la figure 5-8 des sources) :

- **Sélectionner "Ajouter un fichier image"** : Cliquez sur ce bouton pour lancer l'importation.
- **Indiquer l'emplacement** : Saisissez le chemin complet vers le fichier .raw.
- **Choisir le type et la méthode** : Vous devez préciser s'il s'agit d'un disque ou d'une partition et choisir une méthode d'importation (lien symbolique, copie ou déplacement). Les sources privilégient le **lien symbolique (Symlink)** ou la **copie** pour ne pas altérer l'intégrité de la preuve.

3. Méthodes d'analyse et documentation

Une fois le fichier importé, vous disposez de plusieurs outils pour l'explorer :

- **Organisation** : Il est recommandé de placer les éléments extraits de la RAM dans un **sous-dossier dédié** au sein de votre logiciel de gestion de cas pour éviter toute confusion avec les données du disque dur.

- **Chronologie (Timeline)** : Vous pouvez créer une chronologie de l'activité du fichier pour consigner chaque accès à l'artefact pendant l'analyse.
- **Séquenceur d'événements** : Utilisez-le comme un journal numérique pour documenter vos découvertes au fur et à mesure (ex : identification d'un historique de navigation ou de données récupérées).
- **Notes** : Ajoutez des notes détaillées sur chaque artefact trouvé pour faciliter la rédaction ultérieure du rapport d'expertise.

Les sources précisent que si Autopsy est idéal pour débiter car il est gratuit, des **logiciels commerciaux** (comme EnCase ou X-Ways) peuvent offrir davantage d'options pour l'enregistrement et l'analyse approfondie des artefacts. Pour des détails techniques plus poussés sur l'extraction des données, les sources renvoient au **chapitre 7** de l'ouvrage de référence.

Comment capturer la RAM sous Linux ?

Bien que les sources fournies ne détaillent pas les commandes Linux spécifiques pour l'extraction (celles-ci étant traitées au **chapitre 7** de l'ouvrage de référence), elles établissent les principes fondamentaux et le cadre technique pour effectuer cette capture.

Voici comment procéder selon les sources :

1. Principes de capture

- **Maintenir l'état d'alimentation** : Il est impératif de ne pas éteindre ou redémarrer le système Linux avant la capture. La RAM contient des données qui sont **définitivement perdues** en cas de coupure de courant.
- **Priorité absolue** : Selon l'ordre de volatilité de l'IETF (RFC 3227), la mémoire vive occupe la **deuxième position** (juste après les registres et le cache du processeur). Elle doit donc être capturée avant toute analyse de disque ou de fichiers temporaires.

2. Format et extraction

- **Le « dump » RAM** : La capture consiste à extraire le contenu de la mémoire sous la forme d'un fichier image, généralement un **dump RAM au format .raw**.

- **Outils mentionnés** : Bien que les sources ne listent pas les outils de capture Linux (comme LiME ou AVML), elles mentionnent que **Kali Linux** est utilisé comme système de laboratoire et inclut des outils d'analyse forensique. Pour la manipulation de données brutes sous Linux, la commande **dd** est citée comme outil en ligne de commande (bien que l'exemple fourni concerne l'effacement sécurisé d'une clé USB).

3. Gestion et organisation de la capture

Une fois le fichier .raw obtenu, la procédure recommandée est la suivante :

- **Organisation rigoureuse** : Créez un **dossier dédié à la RAM** dans votre logiciel de gestion de cas (comme Autopsy) pour éviter de mélanger ces données avec celles provenant des disques durs.
- **Importation pour analyse** : Le fichier .raw peut être importé dans **Autopsy** en tant que « fichier image » pour y rechercher des preuves de logiciels malveillants ou des processus en cours.
- **Documentation** : Chaque étape de la capture doit être consignée dans un **journal numérique** ou un séquenceur d'événements pour garantir l'admissibilité juridique de la preuve.

Il est essentiel de noter que la capture de la RAM est souvent le seul moyen d'identifier des **logiciels malveillants** qui ne s'installent jamais sur le disque dur.

Peut-on automatiser l'ordre de volatilité ?

Selon les sources, l'automatisation n'est pas directement mentionnée comme une méthode pour exécuter l'ordre de volatilité, mais elle apparaît comme une caractéristique d'une pratique médico-légale parvenue à un haut niveau de maturité.

Voici les points clés à retenir sur ce sujet :

- **L'automatisation comme indicateur de maturité** : Dans le modèle d'évaluation de la pratique médico-légale (basé sur l'IEEE), le **Niveau 4 est défini comme « Mesuré et automatisé »**. À ce stade, l'organisation utilise des progiciels pour automatiser certains objectifs, comme la surveillance, et fixer des échéances précises.

- **Adaptation manuelle nécessaire** : Les sources soulignent que l'enquêteur peut **adapter l'ordre de collecte** en fonction des besoins spécifiques de l'enquête ou de l'effort requis. Par exemple, si la RAM d'un système semble peu pertinente par rapport au disque dur d'un suspect, l'enquêteur peut choisir de prioriser ce dernier.
- **Responsabilité de l'enquêteur** : Le respect de l'ordre de volatilité (des registres/cache vers les supports d'archivage) est présenté comme une **règle fondamentale** que l'enquêteur doit suivre pour éviter la perte de données précieuses et la contamination des preuves.
- **Outils de gestion** : Bien que des logiciels comme **Autopsy** facilitent la gestion du dossier et la consignation des événements, ils servent d'outils d'accompagnement pour l'enquêteur plutôt que d'automates de collecte.

En résumé, si la gestion globale d'une pratique médico-légale peut être automatisée pour gagner en efficacité, la collecte des données volatiles reste une tâche stratégique sous la responsabilité de l'enquêteur, qui doit l'ajuster selon le contexte de chaque affaire.

Quels sont les détails d'un rapport médico-légal ?

Le rapport médico-légal (ou rapport d'expertise judiciaire) est l'élément le plus visible d'une enquête numérique et doit être rédigé avec un soin extrême, car son ton et sa précision peuvent influencer considérablement l'issue d'une affaire.

Selon les sources, un rapport professionnel doit inclure au minimum les sections suivantes :

- **Résumé de l'affaire** : Cette section doit être concise et expliquer **pourquoi** vous avez été sollicité ainsi que les preuves numériques à analyser. Elle ne doit pas inclure les résultats de l'enquête, mais simplement poser le contexte.
- **Acquisition et préparation de l'examen** : Vous devez y détailler toutes les étapes d'interaction avec les preuves, depuis le début de la **chaîne de possession** jusqu'aux mesures de sécurité pour éviter la contamination. Il est crucial d'y mentionner les **valeurs de**

hachage des copies, les outils utilisés et la protection en écriture appliquée.

- **Constatations** : C'est généralement la partie la plus longue. Elle détaille les actions menées et les résultats obtenus. Chaque élément trouvé doit être mis en évidence en précisant la **méthode employée** pour le découvrir, afin de ne laisser aucune place au doute raisonnable.
- **Conclusion** : Elle résume les conclusions basées exclusivement sur les **faits**. L'enquêteur doit relier ses constatations à ce qui s'est produit, sans inclure de sentiments ou de convictions personnelles. Les résultats présentés doivent être **reproductibles**.
- **Liste des auteurs** : Elle indique qui a rédigé le rapport, leurs coordonnées et inclut une section de **signatures** pour authentifier le document. Il est également recommandé d'y ajouter une brève biographie des enquêteurs pour démontrer leur expertise.

Recommandations de rédaction

Pour garantir l'efficacité du rapport, les sources préconisent de suivre ces principes :

1. **Adaptation au public** : Le rapport doit être compréhensible par des non-experts, tels que des gestionnaires, des responsables RH ou des juges. Il est essentiel d'expliquer chaque acronyme technique ou d'inclure une annexe explicative.
2. **Objectivité absolue** : Ne rapportez que des faits vérifiables et évitez toute supposition que vous ne pouvez étayer par des preuves tangibles.
3. **Utilisation d'annexes** : Pour ne pas alourdir le corps du rapport, placez les détails techniques complexes, les photographies et les documents de référence dans des annexes.
4. **Traçabilité** : Le rapport doit être suffisamment détaillé pour que l'enquêteur puisse s'en souvenir parfaitement et l'expliquer même un an après les faits lors d'un procès.

Enfin, des sections optionnelles comme une **table des matières**, un **glossaire de termes**, ou une **chronologie de l'enquête** peuvent être ajoutées selon le style de l'enquêteur ou les exigences de l'organisation.

Quelle est la structure d'une conclusion factuelle ?

La conclusion d'un rapport médico-légal doit être rigoureusement structurée pour transformer les observations techniques en une **synthèse factuelle et irréfutable**. Les éléments structurants d'une telle conclusion reposent sur les principes suivants :

- **Rapport exclusif des faits** : La conclusion ne doit contenir aucune supposition non étayée et se concentrer uniquement sur les faits recueillis durant l'enquête.
- **Mise en corrélation** : L'enquêteur doit relier chaque détail des constatations à la démonstration de ce qui s'est réellement produit (ou non) lors de l'incident.
- **Synthèse et référencement** : Elle offre un résumé des preuves tout en faisant systématiquement référence à la section « **Constatations** » du rapport pour justifier les méthodes employées.
- **Objectivité et neutralité absolue** : Le ton doit rester neutre, sans expression de sentiments ou de convictions personnelles, afin que les preuves parlent d'elles-mêmes.
- **Démonstration de reproductibilité** : L'enquêteur doit démontrer que ses conclusions sont reproductibles et ne nécessitent aucune technique secrète ou particulière pour être confirmées par un tiers.
- **Formulation de l'avis (si nécessaire)** : Si l'on demande de confirmer ou réfuter un acte précis, l'avis doit être formulé en s'appuyant explicitement sur des preuves présentées comme une **source objective**.

En pratique, une conclusion factuelle efficace comprend généralement une **liste des éléments identifiés**, leur **validation** par une autorité compétente (ex : authentification de documents sensibles), et une description précise des artefacts trouvés (ex : courriels, historiques de navigation) étayée par des références directes aux images de preuves ou aux annexes.

Quels types d'appareils bloquent l'écriture ?

Selon les sources, il existe principalement trois catégories de dispositifs ou de solutions pour assurer le blocage en écriture, essentiel à la préservation de l'intégrité des preuves :

- **Les dispositifs matériels dédiés** : Le **Logicube-MD5** est cité comme un exemple spécifique de bloqueur d'écriture physique pour les disques durs.
- **Les duplicateurs de disques portables** : Certains modèles de duplicateurs intègrent directement une fonctionnalité de **blocage en écriture**.
- **Les solutions logicielles** : Il s'agit de **logiciels de blocage en écriture** installés sur les ordinateurs portables d'enquête (sous Windows ou Linux), permettant de protéger les données dès la connexion d'un support suspect.

L'utilisation de ces outils intervient généralement juste avant la création des copies numériques, par exemple lorsqu'un analyste se connecte au disque d'origine via un câble USB pour en extraire les données sans risquer de les modifier.

Comment protéger un disque en écriture ?

Selon les sources, la protection en écriture est une étape indispensable pour garantir l'intégrité des preuves et éviter toute **contamination** qui pourrait invalider une enquête devant les tribunaux.

Il existe trois méthodes principales pour protéger un disque :

- **Les dispositifs matériels dédiés (bloqueurs d'écriture)** : Ce sont des périphériques physiques spécialisés, comme le **Logicube-MD5**, qui s'interposent entre le disque suspect et l'ordinateur de l'enquêteur.
- **Les duplicateurs de disques portables** : Certains modèles de duplicateurs intègrent directement une fonction de **blocage en écriture** lors de la création de copies.

- **Les solutions logicielles** : Il est possible d'utiliser des **logiciels de blocage en écriture** installés directement sur l'ordinateur portable d'investigation (sous Windows ou Linux).

Procédure et importance : L'enquêteur doit impérativement activer cette protection **avant toute interaction** avec le disque original ou sa copie. Par exemple, une procédure standard consiste à activer le blocage en écriture sur la machine d'analyse, puis à se connecter au disque d'intérêt via un câble USB pour procéder à la création des copies numériques sécurisées.

Enfin, toutes les mesures de protection appliquées doivent être scrupuleusement consignées dans le **rapport d'expertise judiciaire** (outils utilisés, moment de l'activation) pour prouver qu'aucune altération n'a eu lieu.

Peut-on utiliser Kali Linux pour capturer la RAM ?

Bien que les sources ne décrivent pas d'outil natif de Kali Linux spécifiquement pour l'acte technique de **capture** (extraction) de la RAM, elles confirment que Kali Linux joue un rôle central dans ce processus en tant qu'environnement de travail.

Voici comment Kali Linux intervient selon les sources :

- **Système de laboratoire** : Kali Linux est présenté comme le **système de laboratoire recommandé** pour mener les tâches d'ingénierie médico-légale.
- **Outils d'analyse** : Kali inclut la suite **Autopsy**, qui permet d'importer et d'analyser des captures de mémoire vive, telles que des **dumps RAM au format .raw**. L'enquêteur peut ainsi explorer le contenu de la RAM pour y trouver des preuves de logiciels malveillants ou des processus actifs.
- **Kit d'intervention** : Pour un premier intervenant, les sources recommandent d'avoir dans son sac d'intervention un **CD ou une clé USB Live de Kali**.
- **Outils réseau** : Kali propose également des outils comme **Nmap** pour découvrir des appareils sur un réseau, ce qui fait partie de l'inventaire préliminaire avant la capture des données.

Il est important de noter que si Kali Linux est le système privilégié pour l'analyse, les sources précisent que les **procédures d'extraction technique** (les commandes spécifiques pour créer le fichier .raw depuis un terminal) sont détaillées dans le **chapitre 7** de l'ouvrage de référence, lequel n'est pas intégralement reproduit ici.

En résumé, vous utilisez Kali Linux pour **gérer l'enquête et analyser le dump**, tandis que la capture elle-même nécessite des outils d'extraction dont les détails techniques sont approfondis plus loin dans l'ouvrage.

Comment faire un journal papier ?

L'utilisation d'un **journal papier** est vivement recommandée par les sources en complément d'un journal numérique pour plusieurs raisons stratégiques. Voici comment le constituer et l'utiliser efficacement selon les meilleures pratiques d'enquête :

1. Utilité et flexibilité

Le journal papier est l'outil privilégié pour la **réactivité immédiate**. Il permet de prendre des notes rapides dès l'arrivée sur les lieux, sans subir les délais techniques comme le temps de démarrage d'un ordinateur portable. Il offre également une liberté totale pour **dessiner des croquis** de l'incident ou de la scène de crime, ce qui est essentiel pour documenter l'environnement physique.

2. Éléments essentiels à consigner

Dès l'ouverture d'un dossier, vous devez noter systématiquement les informations suivantes dans votre journal :

- **La date et l'heure** précises de chaque observation.
- **Le lieu et la localisation** exacte de l'incident.
- **L'état initial des systèmes** : une description détaillée de chaque élément d'intérêt avant toute interaction.
- **Les personnes présentes** : noms et identifications de toutes les personnes sur les lieux ou susceptibles de témoigner.
- **Le type de support** : préciser si les preuves sont de nature volatile ou non volatile.

3. Méthodologie et validation

Bien qu'il n'existe pas de norme officielle ou de méthode unique pour la prise de notes, les sources insistent sur la rigueur de la documentation.

- **Tout documenter** : Plus vos notes sont exhaustives, plus votre futur rapport d'expertise sera pertinent et difficile à contester par la partie adverse.
- **Horodatage et validation** : Chaque élément inscrit doit être horodaté et **validé par l'enquêteur** pour garantir son authenticité.
- **Traçabilité** : Le journal doit refléter la chronologie exacte de votre implication, ce qui est crucial si vous devez expliquer vos actions lors d'un procès des mois ou des années plus tard.

4. Complémentarité avec d'autres outils

Le journal papier ne doit pas être utilisé seul. Il gagne à être complété par :

- **Un journal numérique** (comme le séquenceur d'événements dans Autopsy) pour organiser les preuves extraites.
- **Un enregistreur vocal** pour capturer des notes verbales rapides pendant que vous manipulez des équipements.
- **Des photographies et vidéos** qui viennent appuyer les croquis réalisés à la main.

En résumé, votre journal papier est la mémoire vive de l'enquête de terrain ; il doit être suffisamment détaillé pour permettre à un tiers (ou à vous-même dans le futur) de reconstituer précisément l'état de la scène et vos premières constatations.

Pourquoi utiliser un hub plutôt qu'un commutateur ?

Dans le cadre d'une intervention médico-légale, les sources recommandent d'inclure dans le sac d'intervention un **hub à quatre ports plutôt qu'un commutateur (switch)**.

Bien que les sources ne détaillent pas les caractéristiques techniques intrinsèques de ces deux appareils, cette recommandation s'inscrit dans les principes fondamentaux de l'enquête numérique décrits dans les documents :

1. Capture des empreintes numériques et des paquets

L'un des objectifs majeurs de l'enquête est de **capturer les empreintes numériques** laissées par les appareils et de réaliser des **captures de paquets** pour analyser les échanges réseau.

- **Le problème du commutateur** : Un commutateur est conçu pour diriger le trafic uniquement vers le port de destination spécifique. Pour qu'un enquêteur puisse "voir" le trafic d'un autre appareil sur un commutateur, il devrait généralement modifier la configuration de celui-ci (par exemple, en activant le "port mirroring").
- **L'avantage du hub** : Un hub diffuse par nature tout le trafic qu'il reçoit sur l'ensemble de ses ports. En insérant un hub entre un appareil suspect et le réseau, l'enquêteur peut brancher son ordinateur portable d'analyse sur un autre port du hub et intercepter l'intégralité du trafic sans aucune configuration logicielle.

2. Respect de la "Règle d'or" (Non-contamination)

La règle principale est de **ne jamais modifier l'original** ou l'état du système.

- Toute modification de configuration sur un équipement réseau de production (comme un commutateur) pourrait être considérée comme une **contamination des preuves**, compromettant leur validité légale.
- L'utilisation d'un hub est une méthode physique qui permet d'extraire des données et d'analyser l'empreinte numérique **sans perturber le fonctionnement de l'équipement** ni modifier son état logique.

3. Simplicité et rapidité d'intervention

Le premier intervenant doit être capable de documenter l'état actuel de la zone rapidement. Un hub est un outil "plug-and-play" qui ne nécessite pas de temps de démarrage complexe ou de compétences d'administration réseau avancées pour fonctionner, contrairement à certains commutateurs administrables qui pourraient retarder la collecte de données volatiles.

En résumé, le hub est privilégié car il permet une **écoute passive et totale du trafic réseau**, garantissant ainsi une collecte de preuves complète tout en respectant l'impératif de ne pas altérer l'environnement technique d'origine.

Comment prouver la reproductibilité ?

Pour prouver la reproductibilité de vos constatations lors d'une enquête médico-légale, vous devez démontrer qu'un tiers pourrait obtenir les mêmes résultats en suivant votre méthodologie. Selon les sources, cela repose sur une **transparence totale et une documentation rigoureuse** tout au long du processus.

Voici les éléments clés pour garantir et prouver cette reproductibilité :

- **Détailler la méthodologie d'acquisition** : Dans votre rapport, vous devez consigner précisément chaque étape de l'interaction avec les preuves. Cela inclut les outils utilisés (par exemple, Digital Forensic Framework ou EnCase), les mesures de protection en écriture appliquées et l'utilisation de **valeurs de hachage** pour valider que les copies sont identiques à l'original.
- **Documenter chaque constatation** : La section « Constatations » de votre rapport doit mettre en évidence chaque élément trouvé en précisant la **méthode exacte employée** pour le découvrir. L'objectif est de ne laisser aucune place au doute raisonnable quant à la validité technique de vos conclusions.
- **Éviter les techniques propriétaires ou « secrètes »** : Pour que les preuves soient jugées reproductibles, elles ne doivent nécessiter **aucune technique particulière ou secrète** pour apparaître. Un autre expert doit pouvoir utiliser des outils standards pour confirmer vos découvertes.
- **S'appuyer sur des journaux d'enquête complets** : L'utilisation d'un logiciel de gestion de dossiers (comme Autopsy) est cruciale, car il permet d'extraire des captures d'écran, des notes et des séquences d'événements qui prouvent la démarche suivie. Ces rapports doivent être assez détaillés pour que vous puissiez expliquer vos actions même des années après les faits.
- **Viser un haut niveau de maturité organisationnelle** : Selon le modèle de maturité de l'IEEE cité dans les sources, le **Niveau 3 (« Déploiement complet »)** est atteint lorsque les processus mis en œuvre sont systématiquement reproductibles et offrent la même valeur ajoutée, peu importe le lieu ou le moment de l'enquête.

En résumé, la reproductibilité se prouve par la capacité de votre rapport à servir de « guide » factuel permettant de recréer l'intégralité de l'analyse sans ambiguïté.

Qu'est-ce qu'une cage de Faraday ?

Une **cage de Faraday** est un dispositif ou un conteneur utilisé lors des enquêtes médico-légales numériques pour **bloquer les communications sans fil et cellulaires**.

Selon les sources, son rôle est crucial pour les raisons suivantes :

- **Isolation des signaux** : Elle est conçue pour empêcher un appareil (comme un téléphone mobile) d'échanger des données via Wi-Fi ou les réseaux cellulaires.
- **Préservation des preuves** : En isolant l'appareil, l'enquêteur empêche toute modification ou suppression de données à distance par un tiers, permettant ainsi de conserver le **dernier état de connexion** du système.
- **Intégration et coût** : Cette technologie peut être intégrée à certains **sacs de protection** spécialisés (souvent appelés sacs pour matières dangereuses ou antistatiques) ou prendre la forme d'un conteneur de stockage dédié. Un sac équipé d'une cage de Faraday coûte environ 70 \$ US.

Dans la pratique, l'utilisation d'une cage de Faraday est une étape recommandée pour « éliminer la technologie cloud de l'équation » en désactivant physiquement l'accès aux réseaux sans fil dès la saisie de l'appareil.

Comment fonctionne la chaîne de traçabilité ?

La **chaîne de traçabilité** (ou chaîne de possession) est le processus rigoureux qui documente le cycle de vie complet d'un artefact, de sa découverte initiale jusqu'à sa restitution ou sa destruction finale. Son objectif principal est de garantir l'**authenticité des preuves** et d'éliminer tout risque de contestation lié à une éventuelle contamination par une partie adverse.

Voici comment elle fonctionne concrètement selon les sources :

1. Documentation de l'état initial

Le processus commence avant même la première interaction physique avec l'objet. L'enquêteur doit consigner l'**état initial du système** en

détail à l'aide de vidéos, de photographies et d'un journal d'enquête. Cette étape permet d'identifier clairement l'appareil parmi d'autres objets similaires et de reconnaître ses fonctionnalités au moment de la saisie.

2. Ensachage et Étiquetage

Une fois saisi, chaque artefact doit être manipulé avec soin :

- **Protection physique** : L'utilisation de **sacs antistatiques** ou pour matières dangereuses est recommandée pour protéger les composants électroniques des charges statiques. Pour les appareils mobiles, une **cage de Faraday** est nécessaire pour bloquer les communications sans fil.
- **Étiquetage systématique** : Chaque sac doit porter une étiquette mentionnant la date et l'heure de la saisie, les numéros de série, les caractéristiques uniques de l'actif et le nom de la personne chargée de la collecte.

3. Suivi des accès et stockage

La traçabilité repose sur un enregistrement ininterrompu de chaque mouvement de la preuve :

- **Registre des mouvements** : Chaque fois qu'un artefact est consulté, déplacé ou analysé, une entrée doit être créée dans un registre numérique (souvent via un logiciel de gestion de cas comme Autopsy).
- **Salle des scellés** : Lorsqu'ils ne sont pas activement examinés, les artefacts doivent être conservés dans un lieu de stockage sécurisé, appelé **salle des scellés**.
- **Responsabilité** : Le registre doit préciser l'identité de chaque personne ayant eu accès à l'élément, garantissant que la responsabilité est clairement établie à chaque étape.

4. Clôture et destination finale

À la fin de l'implication de l'enquêteur, la chaîne doit être bouclée de manière formelle :

- Les éléments sont soit **restitués au propriétaire**, soit **détruits** de manière sécurisée (par exemple, par perçage des plateaux d'un disque dur).
- L'identité de la dernière personne ayant accédé à l'élément avant sa restitution ou sa destruction doit être scrupuleusement documentée pour éviter toute accusation de mauvaise gestion ultérieure.

Le non-respect de cette procédure, comme l'omission d'un transfert dans le registre ou une surveillance interrompue de la zone, peut être interprété comme une **opportunité de contamination** et conduire au rejet des preuves par un tribunal.

Comment documenter les horodatages ?

La documentation des horodatages est une composante essentielle de la rigueur d'une enquête médico-légale numérique pour garantir l'intégrité et la validité des preuves. Selon les sources, voici comment procéder :

1. Principes généraux de documentation

- **Systématisation** : Chaque élément documenté pour décrire l'environnement de l'enquête doit être impérativement **horodaté et validé par l'enquêteur**.
- **Ouverture du dossier** : Dès le début de l'investigation, la date et l'heure précises de l'ouverture du dossier, ainsi que celles de l'incident, doivent être consignées.
- **Étiquetage physique** : Pour chaque artefact saisi, l'enquêteur (ou la personne chargée de la collecte) doit inscrire la **date et l'heure actuelles** directement sur le sac de scellé.

2. Éléments techniques spécifiques

- **Dérive de l'horloge** : Il est crucial de noter et d'enregistrer toute **dérive de l'horloge système** des appareils analysés. Cela permet de recréer une chronologie exacte des événements malgré les décalages possibles entre les systèmes.
- **Preuves réseau** : Tous les enregistrements collectés sur un réseau (journaux, tables de routage, etc.) doivent être horodatés et étiquetés selon leur emplacement sur le schéma réseau.
- **Capture de la RAM** : Étant donné que les données volatiles changent en nanosecondes, il est nécessaire de capturer et d'étiqueter ces données en partant du principe qu'une capture ultérieure sera différente.

3. Utilisation d'outils numériques

- **Séquenceur d'événements** : Les logiciels de gestion de cas comme Autopsy permettent d'utiliser un séquenceur d'événements

pour agir comme un **journal numérique**. Chaque accès à un artefact ou chaque découverte doit y être consigné avec sa date et son heure.

- **Rapport de chronologie (Timeline)** : L'analyse peut inclure la création d'une chronologie de l'activité des fichiers, permettant de visualiser chaque accès aux données au fil du temps.
- **Suivi du temps de travail** : Pour la clôture du dossier et la facturation, il est recommandé d'enregistrer les heures de travail et la date précise de fin d'implication via des outils comme TimeLive.

En résumé, la documentation des horodatages ne se limite pas à noter l'heure d'une découverte ; elle englobe la synchronisation technique (dérive de l'horloge), la traçabilité physique (étiquettes) et le suivi chronologique continu de toutes les actions de l'enquêteur.

Rôle du premier intervenant ?

Le premier intervenant (ou *first responder*) joue un rôle charnière dans une enquête médico-légale numérique, car c'est de ses actions initiales que dépend la validité juridique des preuves collectées. Il n'est pas forcément la première personne physiquement arrivée sur les lieux, mais celle qui **identifie la nécessité d'une enquête**.

Voici les responsabilités et missions spécifiques du premier intervenant selon les sources :

1. Préservation et sécurisation de la scène

La priorité absolue est d'éviter la contamination des preuves :

- **Isoler la zone** : Il doit mettre la zone en quarantaine pour empêcher toute intervention non autorisée.
- **Sécurisation physique** : L'utilisation de ruban de signalisation (« Zone interdite ») est recommandée pour marquer le périmètre.
- **Surveillance continue** : La zone doit être surveillée sans interruption jusqu'à l'arrivée des experts. Toute rupture de surveillance peut être interprétée comme une opportunité de contamination.

2. Documentation exhaustive (L'état des lieux)

Le premier intervenant doit figer l'état de la scène avant toute interaction technique :

- **Inventaire des actifs** : Établir une liste complète des appareils concernés (avec numéros de série) et classer leur volatilité.
- **Photographie et vidéo** : Capturer l'état actuel des systèmes, y compris les éléments affichés à l'écran, les périphériques connectés et les câbles réseau branchés.
- **Horodatage et validation** : Chaque observation, croquis ou photo doit être **horodaté et validé** par l'enquêteur.
- **Collecte d'informations** : Recueillir les noms et coordonnées des témoins potentiels.

3. Évaluation et coordination

- **Analyse des menaces** : Évaluer les dangers ou menaces qui pourraient peser sur le bon déroulement de l'enquête.
- **Alerte et contact** : Prévenir l'équipe de réponse aux incidents et contacter les parties externes (autorités, propriétaires des données).
- **Décision stratégique** : Évaluer l'effort requis et décider si l'enquête peut être menée en interne ou si elle doit être sous-traitée.

4. Matériel d'intervention (*Sac d'intervention*)

Pour mener à bien sa mission, le premier intervenant doit disposer d'un équipement prêt à l'emploi, notamment :

- Un ordinateur portable sécurisé (Windows/Linux) et des supports de stockage de grande capacité.
- Des **bloqueurs d'écriture** physiques ou logiciels.
- Un **hub à quatre ports** (plutôt qu'un commutateur) pour capturer le trafic réseau sans configurer les équipements de production.
- Des formulaires de **chaîne de possession**, des étiquettes et un enregistreur vocal.

En résumé, le succès d'une enquête repose souvent sur la formation du premier intervenant : s'il ne suit pas les procédures adéquates de documentation et d'isolation, la collecte des preuves risque d'échouer ou d'être invalidée devant un tribunal.

Comment documenter la dérive d'horloge ?

La documentation de la dérive d'horloge système est une étape obligatoire pour garantir l'intégrité de la chronologie des faits. Selon les sources, voici les modalités pour la documenter :

- **Inscription dans l'état des lieux** : La dérive de l'horloge fait partie de la liste des éléments courants à consigner pour garantir une documentation complète de l'environnement étudié.
- **Validation par l'enquêteur** : Chaque enregistrement concernant la dérive d'horloge doit être impérativement **horodaté et validé** par l'enquêteur au moment de la constatation.
- **Utilisation d'un journal numérique** : Il est fortement recommandé de consigner cette information dans un **logiciel de gestion de cas** (comme Autopsy, DFF ou EnCase). Vous pouvez utiliser le **séquenceur d'événements** pour créer une entrée spécifique indiquant le décalage constaté entre l'heure du système analysé et l'heure réelle de référence.
- **Intégration au rapport final** : Cette donnée doit figurer dans la section « **Acquisition et préparation de l'examen** » de votre rapport médico-légal. Vous devez y détailler l'état du système lors de la prise en charge pour permettre aux lecteurs (ou à la partie adverse) de comprendre comment la chronologie des événements a été reconstituée.

Pourquoi est-ce crucial ? Documenter cette dérive est indispensable pour synchroniser les artefacts provenant de sources différentes (journaux réseau, fichiers système, etc.) et prouver que votre analyse est **fiable et reproductible** devant un tribunal. Sans cette précision, la validité de votre chronologie des événements pourrait être contestée.

Quels logiciels utiliser pour l'analyse ?

Pour l'analyse médico-légale et la gestion de cas, les sources recommandent plusieurs logiciels, allant d'outils gratuits à des suites commerciales professionnelles.

Logiciels de gestion de cas et d'analyse forensique

Le choix du logiciel dépend souvent du budget et du style d'enquête de l'analyste. Les options mentionnées sont :

- **Autopsy** : C'est l'outil gratuit privilégié par les sources car il est disponible nativement sous **Kali Linux**. Il sert à la fois d'outil d'analyse pour les images disque et de plateforme de gestion de cas (journalisation, notes, chronologie).
- **Digital Forensic Framework (DFF)** : Un outil utilisé pour l'analyse et l'extraction de données, notamment pour l'historique de navigation ou les registres.
- **EnCase** (Guidance Software) : Une solution commerciale populaire recommandée pour un usage professionnel.
- **X-Ways Forensics** : Une autre option commerciale robuste citée pour les enquêtes professionnelles.
- **Open Computer Forensics Architecture (OCFA)** : Une alternative mentionnée pour la gestion de cas.
- **WinHex** : Utilisé spécifiquement pour l'examen technique des copies de disques.

Outils d'investigation réseau

Pour analyser l'empreinte numérique sur un réseau ou découvrir des périphériques, les outils suivants sont suggérés :

- **Nmap (Network Mapper)** : L'outil de référence sous Kali Linux pour cartographier un réseau et identifier les systèmes d'exploitation.
- **Angry IP Scanner** : Un scanner d'adresses IP permettant d'exporter les résultats vers le dossier d'enquête.
- **Wireshark et SNORT** : Utilisés pour l'analyse approfondie du trafic et la détection d'attaques.
- **Draw.io, LucidChart ou Dia Diagram** : Logiciels servant à schématiser la topologie du réseau analysé.

Outils spécialisés et utilitaires

D'autres logiciels remplissent des fonctions précises durant le cycle de vie de l'enquête :

- **TimeLive** : Pour le suivi des heures de travail et la facturation.
- **Eraser** ou **Darik's Boot and Nuke (DBAN)** : Pour la suppression sécurisée et définitive des données de niveau forensique.
- **Cisco CloudLock** : Un exemple de tableau de bord CASB pour surveiller les événements de sécurité dans le cloud.

Les sources soulignent qu'il est préférable d'utiliser ces logiciels spécialisés plutôt qu'un simple bloc-notes papier, car ils facilitent la documentation, la reproductibilité et la génération de rapports professionnels. Avez-vous besoin de plus de détails sur l'un de ces logiciels ?

Peut-on analyser l'historique web avec Autopsy ?

Oui, il est tout à fait possible d'analyser l'**historique web** avec **Autopsy**. Selon les sources, Autopsy est une suite d'outils utilisée principalement pour **analyser les images disque** collectées lors d'une enquête. Voici comment l'historique web est traité dans ce cadre :

- **Identification des artefacts** : Dans les exemples fournis par les sources, le séquenceur d'événements d'Autopsy montre explicitement l'identification d'artefacts liés à la navigation, comme **l'historique du navigateur Firefox**.
- **Visualisation et organisation** : Le logiciel permet de mettre en évidence des dossiers spécifiques contenant l'historique de navigation. Ces découvertes peuvent ensuite être documentées dans le rapport d'expertise pour illustrer les **sites web consultés** par le système analysé.
- **Chronologie (Timeline)** : Autopsy permet de créer une chronologie de l'activité des fichiers, ce qui aide à consigner chaque accès aux artefacts web pendant l'analyse.

Bien que les sources mentionnent qu'Autopsy est un outil gratuit et performant disponible sous Kali Linux, elles précisent que des logiciels commerciaux pourraient offrir encore plus d'options pour l'enregistrement et la gestion de ces artefacts.

Comment documenter les découvertes dans Autopsy ?

Dans Autopsy, la documentation des découvertes s'effectue de manière structurée pour servir de **journal de criminalistique numérique**. Voici les méthodes spécifiques recommandées par les sources :

- **Le Séquenceur d'événements (Event Sequencer)** : C'est l'outil privilégié pour consigner vos découvertes au fur et à mesure de l'analyse. Il permet d'enregistrer des événements précis en indiquant la date, l'heure, la source et une note descriptive (par exemple, l'identification d'un historique de navigation Firefox ou de données récupérées dans la corbeille).
- **La prise de notes intégrée** : Vous pouvez ajouter des **notes** directement associées aux images ou aux artefacts analysés. Ces notes, accompagnées de captures d'écran, peuvent être extraites ultérieurement pour justifier vos conclusions dans le rapport d'expertise judiciaire.
- **La Chronologie (Timeline)** : Autopsy permet de générer une chronologie de l'activité des fichiers, ce qui aide à documenter chaque accès à un artefact durant l'analyse.
- **Organisation hiérarchique** : Il est conseillé d'organiser le journal selon une relation **parent/enfant**, où chaque nouvel élément découvert est considéré comme un « enfant » de l'élément source dont il provient. Par exemple, les artefacts extraits de la RAM devraient être regroupés dans un dossier spécifique au sein du logiciel pour éviter toute confusion avec les données du disque dur.
- **Exportation des preuves** : Une fois l'enquête terminée, les données des outils de journalisation et les rapports chronologiques peuvent être **exportés** pour être joints au rapport final, prouvant ainsi la rigueur de la démarche d'enquête.

Les sources précisent que bien qu'Autopsy soit un excellent outil gratuit pour illustrer ces concepts, des logiciels commerciaux peuvent offrir des options de documentation et d'enregistrement des artefacts encore plus performantes.

Comment consigner un transfert de responsabilité ?

La consignation d'un **transfert de responsabilité** est une étape critique de la chaîne de traçabilité, car elle garantit que chaque mouvement d'une preuve est documenté et qu'aucune période n'est laissée sans surveillance, ce qui prévient toute contestation pour contamination.

Voici comment consigner ce transfert selon les sources :

- **Déclenchement immédiat de la documentation** : Votre documentation propre doit commencer **dès l'instant précis du transfert de responsabilité**. Tous les dossiers créés à partir de ce moment doivent intégrer les informations recueillies lors du passage de relais.
- **Entretien avec l'intervenant précédent** : Vous devez consigner les **hypothèses et les détails** obtenus lors de votre entretien avec le ou les premiers intervenants. Cela permet de comprendre les actions survenues avant votre arrivée.
- **Identification complète des acteurs** : Il est impératif de recueillir et de noter les **coordonnées complètes** de l'équipe d'intervention initiale et de chacun de ses membres. Chaque information obtenue doit être **étiquetée avec le nom de la personne** qui l'a fournie.
- **Utilisation de registres formels** :
 - **Formulaires physiques** : Utilisez des formulaires de **chaîne de possession** (comme le modèle du NIST) pour enregistrer officiellement qui remet l'objet et qui le reçoit, avec signatures et horodatages.
 - **Registres numériques** : Chaque fois qu'un artefact est consulté ou déplacé après le transfert, une entrée doit être créée dans un **registre numérique** (via un logiciel comme Autopsy).
- **Consignation de la fin d'implication** : Lorsque vous transférez à votre tour la responsabilité (à la clôture du dossier ou pour stockage), vous devez documenter vos **périodes d'activité exactes** et l'identité de la **dernière personne ayant accédé** aux éléments.

Le respect rigoureux de ces consignes permet d'établir une responsabilité claire et continue, empêchant la partie adverse d'exploiter une éventuelle **rupture de la chaîne de possession**.

Pourquoi privilégier les registres ?

L'utilisation de **registres** et de logiciels de gestion de dossiers est privilégiée dans une enquête médico-légale pour plusieurs raisons cruciales touchant à la validité juridique, à l'organisation et à la pérennité de l'enquête :

1. Garantie de l'admissibilité juridique

La documentation systématique dans des registres est indispensable pour prouver l'**authenticité et la fiabilité** des preuves. Les parties adverses cherchent souvent à discréditer les preuves numériques en les présentant comme incomplètes ou altérées ; un registre détaillé permet de rapporter uniquement les faits et d'étayer chaque argument par des détails vérifiables. Sans un registre rigoureux de la **chaîne de traçabilité**, les preuves risquent d'être rejetées par les tribunaux.

2. Gestion de la complexité et de l'organisation

Les enquêtes génèrent souvent une quantité massive de données qui peuvent rapidement devenir **chaotiques** sans une organisation stricte.

L'utilisation de registres numériques permet de :

- Maintenir une relation **parent/enfant** entre les artefacts originaux et les éléments extraits.
- Éviter la perte de fichiers et simplifier l'association des données à leur source.
- Faciliter le **transfert de dossier** à un tiers, puisque toutes les notes y sont déjà consignées.

3. Traçabilité des accès et surveillance

Il est impératif de tenir un registre pour chaque mouvement d'un artefact. Chaque fois qu'une preuve est consultée ou déplacée, le registre doit préciser **qui** y a accédé et **où** elle est stockée. De même, un registre des personnes responsables de la surveillance d'une scène de crime est essentiel pour lever tout doute sur une éventuelle compromission des lieux.

4. Mémoire à long terme de l'enquêteur

Une enquête peut durer longtemps et être portée devant les tribunaux des mois, voire des années plus tard. Les registres permettent à l'enquêteur de :

- Se souvenir parfaitement des faits et des actions menées sans avoir à se fier uniquement à sa mémoire.
- Justifier ses **périodes d'activité** et l'heure exacte de son désengagement du dossier.
- Fournir une base solide pour la rédaction du **rapport d'expertise final**.

5. Professionnalisme et maturité de la pratique

Le recours à des registres automatisés est un indicateur de maturité organisationnelle (Niveau 4 : « Mesuré et automatisé » selon l'IEEE).

Cela permet de mesurer les coûts, de suivre les heures de travail pour la facturation (via des outils comme TimeLive) et de démontrer la valeur de l'équipe médico-légale auprès de la direction.

Comment consigner un hachage ?

La consignation des valeurs de hachage est une procédure essentielle pour garantir l'intégrité des preuves et leur admissibilité juridique. Selon les sources, voici comment procéder :

- **Section dédiée dans le rapport** : Les valeurs de hachage de **chaque copie** numérique doivent être impérativement consignées dans la section « **Acquisition et préparation de l'examen** » du rapport médico-légal.
- **Stockage sécurisé** : Il est recommandé de répertorier et de conserver ces valeurs sur un **système d'investigation isolé** afin de garantir qu'elles ne soient pas altérées.
- **Utilisation de logiciels spécialisés** : L'emploi de logiciels de gestion de cas (tels que **Autopsy**, **DFF** ou **EnCase**) est préconisé pour faciliter la documentation de ces valeurs lors de la création des copies.
- **Preuve de non-contamination** : La validation du hachage sert à démontrer que les copies sont strictement identiques à l'original. Toute modification de la valeur de hachage constatée au cours de l'enquête est considérée comme une **contamination**, ce qui peut entraîner le rejet des preuves par un tribunal.
- **Transparence et reproductibilité** : Consigner ces détails permet de prouver que l'enquêteur a suivi les étapes appropriées pour

identifier les preuves sans les modifier, rendant ainsi les conclusions de l'enquête **fiables et reproductibles** par un tiers.

Qu'est-ce qu'une table de routage ?

Une **table de routage** est un artefact de données présent dans les périphériques réseau et les composants informatiques, contenant des informations sur les chemins de communication entre les appareils. Selon les sources, elle revêt une importance particulière dans une enquête médico-légale pour les raisons suivantes :

- **Haute volatilité** : La table de routage est classée au **deuxième niveau de l'ordre de volatilité** (juste après les registres et le cache du processeur). Cela signifie qu'elle contient des données extrêmement fragiles qui doivent être collectées en priorité.
- **Évolution constante** : Les informations qu'elle contient sont en **constante mutation**. Elles peuvent être modifiées par le système lui-même, même lorsqu'un administrateur n'utilise pas l'équipement.
- **Sensibilité à l'alimentation** : Comme il s'agit de données volatiles, le contenu d'une table de routage est **définitivement perdu en cas de coupure de courant** ou de mise hors tension de l'appareil.
- **Rigueur de collecte** : Lors d'une investigation, les tables de routage doivent être collectées, **horodatées et étiquetées** selon leur emplacement exact sur le schéma du réseau. Elles sont essentielles pour obtenir des preuves sur les échanges entre les périphériques, par opposition aux données extraites directement des ordinateurs des utilisateurs.

Quels sont les niveaux de maturité IEEE ?

Selon les sources, le modèle de maturité de l'**IEEE** pour la criminalistique numérique permet d'évaluer et d'améliorer les compétences d'une organisation en décomposant sa pratique en six niveaux distincts.

Voici les détails de chaque niveau de maturité :

- **Niveau 0 : Pratiques personnelles** : Les tâches de criminalistique sont effectuées, mais elles ne sont **pas documentées**. Il n'existe aucun plan formel, les compétences dépendent uniquement des personnes présentes, et le départ d'un spécialiste signifie souvent la perte totale de l'expertise pour l'organisation.
- **Niveau 1 : Processus documenté** : Une documentation officielle existe et est approuvée, mais elle est **rarement mise à jour**. Cela crée une « dérive de processus » où la pratique réelle de l'équipe ne correspond plus à ce qui est écrit, limitant ainsi les mécanismes de contrôle.
- **Niveau 2 : Déploiement partiel** : Les activités documentées commencent à être déployées, mais de manière **incohérente**. Certaines étapes peuvent être omises ou non documentées, et la qualité des livrables varie selon le lieu ou le moment du travail.
- **Niveau 3 : Déploiement complet** : Il existe une **cohérence parfaite** entre la documentation et les actions sur le terrain. Les processus sont **reproductibles** et offrent la même valeur ajoutée quels que soient l'heure ou le lieu de l'enquête.
- **Niveau 4 : Mesuré et automatisé** : L'organisation fixe des objectifs précis avec des échéances, évalue la satisfaction client et mesure les coûts de réalisation. Ce niveau s'appuie généralement sur des **logiciels de gestion des ressources** pour automatiser le suivi.
- **Niveau 5 : Amélioration continue** : C'est le niveau le plus avancé, où l'objectif n'est plus statique. L'organisation analyse systématiquement les résultats de ses enquêtes pour **adapter ses processus** et ses outils en fonction des pistes d'amélioration identifiées.

L'évaluation selon ce modèle porte sur des aspects variés tels que les personnes, les processus, les outils, la base de connaissances et les profils de compétences. Atteindre les niveaux supérieurs (comme le niveau 4) nécessite souvent l'acquisition de **technologies de surveillance automatisées** ou de logiciels spécialisés.

Pourquoi utiliser le Logicube-MD5 ?

Le **Logicube-MD5** est utilisé comme un **dispositif matériel de blocage en écriture** pour les disques durs. Son utilisation est cruciale pour plusieurs raisons liées à l'intégrité de l'enquête :

- **Protection contre la contamination** : La règle d'or en criminalistique numérique est de ne jamais modifier l'élément original. Le Logicube-MD5 empêche physiquement toute écriture sur le disque suspect, évitant ainsi une **contamination** qui pourrait invalider les preuves devant un tribunal.
- **Intégrité des preuves** : En garantissant qu'aucune donnée n'est altérée lors de la connexion à l'ordinateur de l'enquêteur, il assure que les copies numériques créées sont strictement identiques à l'original.
- **Outil du premier intervenant** : Il fait partie des outils essentiels du **sac d'intervention forensique** que le premier intervenant doit avoir à sa disposition pour sécuriser les preuves dès son arrivée sur les lieux.
- **Documentation et recevabilité** : L'utilisation d'un tel bloqueur d'écriture doit être consignée dans le rapport médico-légal (section « Acquisition et préparation de l'examen ») pour démontrer que l'expert a suivi les procédures appropriées pour identifier les preuves sans les modifier.

En résumé, le Logicube-MD5 est un outil de **sécurisation physique** indispensable pour maintenir la force probante des données numériques collectées.

Quelle est la règle d'or pour préserver les preuves ?

La règle d'or (ou règle principale) absolue en matière d'enquête médico-légale numérique est la suivante : **n'examinez jamais l'élément original**.

Le respect de cette règle est crucial pour les raisons suivantes :

- **Éviter la contamination** : Toute modification apportée à l'artefact original, même involontaire, est considérée comme une contamination qui peut compromettre l'utilisation légale des preuves devant un tribunal.
- **Garantir l'admissibilité** : Si l'appareil original est altéré ou modifié, l'affaire peut être classée sans suite par le système judiciaire.

Procédure standard pour respecter cette règle : Au lieu de travailler sur l'original, l'enquêteur doit impérativement effectuer ces trois étapes sur tout élément numérique collecté avant de commencer son analyse :

1. **Créer plusieurs copies numériques** de l'élément.
 2. **Valider le hachage** de ces copies pour démontrer techniquement qu'elles sont strictement identiques à l'original.
 3. **Activer la protection en écriture** sur la copie avant de l'examiner.
- Cette méthodologie permet de préserver l'intégrité de la source tout en permettant une investigation approfondie sur des duplicata sécurisés.

Quels sont les sept niveaux de volatilité de l'IETF ?

Selon les sources, le classement de la volatilité des preuves numériques s'appuie sur le document **RFC 3227 de l'IETF** (Internet Engineering Task Force). Les données doivent toujours être collectées en priorité selon cet ordre, du plus volatil au moins volatil.

Voici les sept niveaux de volatilité définis :

1. **Registres et Cache** : Il s'agit des registres et du cache du processeur. Ce sont les éléments les plus volatils car ils évoluent en quelques nanosecondes.
2. **Table de routage, Cache ARP, Table des processus, Statistiques du noyau et Mémoire** : Ces données résident dans les périphériques réseau et les composants informatiques. Elles sont en constante évolution et sont définitivement perdues en cas de coupure de courant.
3. **Systèmes de fichiers temporaires** : Ces fichiers peuvent être perdus lors d'une mise hors tension, mais ils ont tendance à persister davantage que les artefacts des niveaux précédents.

4. **Disque** : Les données sur disque (disques durs classiques ou SSD) sont conçues pour être sauvegardées, le risque de perte est donc faible.
5. **Données de journalisation et de surveillance à distance** : Ces journaux sont généralement stockés, mais ils sont plus susceptibles d'être perdus ou altérés que les données d'un disque dur. Ils sont considérés comme moins précieux pour l'enquête.
6. **Configuration physique et topologie réseau** : Ces éléments sont jugés stables et présentent généralement peu d'intérêt pour l'analyse médico-légale immédiate.
7. **Supports d'archivage** : Ce sont les éléments les moins volatils ; il s'agit d'archives anciennes, considérées comme encore moins précieuses que les artefacts récents.

L'enquêteur peut toutefois adapter l'effort de collecte en fonction de la pertinence de l'appareil pour l'enquête. Par exemple, obtenir une copie d'un disque dur peut parfois s'avérer plus crucial que de récupérer la RAM d'un système inutilisé par un suspect.

Comment documenter les personnes présentes ?

La documentation des personnes présentes sur les lieux d'un incident est une étape critique dès l'ouverture d'un dossier médico-légal pour garantir la transparence et la fiabilité de l'enquête. Selon les sources, voici les procédures à suivre :

1. Catégories de personnes à documenter

Il est nécessaire d'identifier et de consigner les informations concernant plusieurs groupes d'individus :

- **Les personnes présentes sur les lieux** : Lors de l'ouverture du dossier, vous devez noter l'identité de toutes les personnes se trouvant sur la scène du crime au moment de votre arrivée.
- **Les témoins potentiels** : Le premier intervenant a pour mission spécifique de recueillir les **noms et identifications** des personnes susceptibles de témoigner ou d'avoir vu l'incident.
- **Les premiers intervenants** : Vous devez établir une liste exhaustive de tous les membres de l'équipe d'intervention initiale, incluant leurs **coordonnées complètes**.

2. Informations et traçabilité

La documentation ne doit pas se limiter à une simple liste de noms ; elle doit permettre un suivi rigoureux :

- **Coordonnées** : Il est impératif de noter les moyens de contact (téléphone, courriel) de chaque personne, au cas où des questions surgiraient ultérieurement sur des actions passées.
- **Attribution des informations** : Chaque détail ou hypothèse recueilli lors d'entretiens doit être **étiqueté avec le nom de la personne** qui a fourni l'information.
- **Validation** : Chaque élément documenté concernant l'environnement (incluant la présence de personnes) doit être **horodaté et validé par l'enquêteur**.

3. Formalisation dans les rapports

Ces informations doivent être intégrées de manière structurée :

- **Logiciel de gestion de cas** : Il est recommandé d'utiliser des outils comme Autopsy pour saisir le nom des enquêteurs et des intervenants impliqués dès la création d'une nouvelle affaire.
- **Rapport d'expertise final** : Le rapport doit inclure une section « Liste des auteurs » mentionnant qui a rédigé le document et les coordonnées des personnes citées.
- **Authentification** : Une section de **signatures** est nécessaire pour authentifier les contributions de chacun au rapport. Il est également suggéré d'inclure une brève biographie des enquêteurs pour démontrer leur expertise.

En résumé, une documentation complète des personnes présentes permet de sécuriser la **chaîne de possession** et de répondre efficacement aux éventuelles contestations de la partie adverse lors d'un procès.

Où trouver des modèles ?

Pour trouver des modèles de documents nécessaires à une enquête médico-légale numérique, les sources suggèrent plusieurs ressources spécifiques selon le type de document recherché :

1. Modèles de rapports d'expertise et de formulaires d'enquête

- **Sites web spécialisés** : Vous pouvez trouver des modèles de rapports forensiques à l'adresse suivante : www.sampletemplates.com/business-templates/forensic-report.html.
- **Logiciels de bureautique** : Il est recommandé d'utiliser des modèles de formulaires d'enquête préétablis avec **Microsoft Word** ou **OneNote**.
- **Organismes officiels** : Le **NIST** (National Institute of Standards and Technology) propose des modèles et des formations pour la déclaration des données.

2. Modèles pour la chaîne de traçabilité

- **NIST** : Cet organisme propose également des exemples de documents de traçabilité pour consigner l'état des preuves et suivre les accès (voir la figure 5-12 des sources).

3. Modèles de demandes de mandats

- **RCFL (Regional Computer Forensics Laboratory)** : Les sources citent des exemples de formulaires de demande de mandat, notamment pour le district du Kansas : www.rcfl.gov/heart-of-america/documents-forms/searchwarrant_computer.doc.
- **Conseil général** : Il est conseillé de consulter en ligne les formulaires de demande de mandat correspondant spécifiquement à votre domaine d'activité ou à votre zone géographique.

4. Logiciels de gestion de cas (Modèles intégrés)

L'utilisation de logiciels de gestion de dossiers comme **Autopsy**, **DFF**, **X-Ways Forensics** ou **EnCase** est vivement encouragée car ils intègrent des structures de rapports et des journaux numériques qui guident l'enquêteur dans la saisie des informations.

En résumé, bien qu'il n'existe pas de norme officielle unique, s'appuyer sur les modèles du **NIST** ou des sites spécialisés permet de garantir que les notes sont suffisamment pertinentes pour ne pas être contestées par la partie adverse.

Quels mandats de perquisition sont requis ?

L'obtention de mandats est une étape juridique cruciale avant de pouvoir accéder à un système et commencer une enquête. Selon les sources, les exigences varient en fonction de la juridiction, mais plusieurs principes généraux s'appliquent :

1. Mandats de perquisition et de saisie

Les principaux documents requis sont les **mandats de perquisition et de saisie**. Ces mandats sont nécessaires pour se prémunir contre toute violation de la législation sur la protection de la vie privée, à moins de disposer d'une autorisation explicite du propriétaire ou que les éléments ne soient visibles publiquement.

2. Étendue et zone géographique

Un mandat n'est pas une autorisation universelle ; il possède des limites précises :

- **Portée spatiale** : Un mandat peut concerner une zone très spécifique, comme une seule pièce, ou être beaucoup plus étendu, englobant l'ensemble d'une entreprise.
- **Limites géographiques** : L'enquêteur doit impérativement s'assurer qu'il travaille dans la **zone géographique exacte** spécifiée par le mandat.
- **Délai de détention** : Les mandats prévoient souvent un délai maximal pour la détention des preuves, qu'il faut respecter pour éviter des complications juridiques.

3. La notion de « Cause probable »

La plupart des systèmes judiciaires exigent une forme de **cause probable** pour délivrer un mandat. Pour que cette cause soit jugée suffisante, l'enquêteur doit se baser sur des **faits incontestables** plutôt que sur des arguments contestables (par exemple, une simple adresse IP peut être jugée insuffisante car elle peut provenir d'un réseau non sécurisé).

4. Nécessité d'un nouveau mandat

Il est fréquent que de nouvelles preuves soient découvertes en cours de route, ce qui peut changer la nature de l'enquête :

- Si un enquêteur découvre des preuves d'un crime différent de celui visé initialement (par exemple, des images pédopornographiques lors d'une enquête sur des stupéfiants), un **nouveau mandat** est généralement nécessaire pour étendre la recherche à ces nouvelles preuves.

5. Cas particuliers et difficultés

- **Cloud** : L'obtention de mandats pour enquêter sur des environnements cloud de grande envergure est jugée particulièrement complexe en raison de la nature décentralisée des données.
- **Entreprises** : Dans de nombreuses entreprises, les employés renoncent à leur droit à la vie privée pour les biens appartenant à l'employeur, ce qui peut simplifier l'accès sans mandat si des accords d'utilisation sont en place.

En résumé, vous devez collaborer avec une équipe juridique pour déterminer le nombre d'éléments couverts, la durée de l'accès autorisée et les types d'artefacts acceptables afin de garantir que l'intégralité du processus est documentée et juridiquement valide.

Accès aux systèmes cloud

L'accès aux systèmes cloud dans le cadre d'une enquête médico-légale présente des défis techniques et juridiques majeurs en raison de la nature décentralisée du traitement des données. Voici les éléments clés concernant cet accès selon les sources :

1. Obstacles à l'accès direct

Contrairement aux enquêtes sur des ressources locales, l'accès physique à l'artefact est souvent impossible car il se trouve dans un centre de données distant. Les cadres d'investigation actuels supposent généralement un accès direct à l'artefact, ce qui n'est pas le cas pour le cloud. Les fournisseurs de services cloud sont souvent **réticents à fournir les données** (journaux d'applications ou de réseau), notamment parce que leur matériel héberge simultanément plusieurs clients qui n'ont aucun lien avec l'enquête.

2. Défis juridiques et mandats

L'obtention de mandats pour enquêter sur des environnements cloud de grande envergure est jugée complexe. La définition des règles d'investigation numérique et de l'étendue des accès qu'un fournisseur doit accorder reste incertaine dans la plupart des systèmes juridiques. De plus, les données peuvent être fragmentées ou multi-juridictionnelles, ce qui peut amener la partie adverse à contester les

preuves en les présentant comme des ouï-dire ou comme étant incomplètes.

3. Stratégie de préservation

Compte tenu de ces difficultés, les sources recommandent de tenter **d'éliminer la technologie cloud de l'équation** dès le début de l'investigation :

- **Désactivation immédiate** : Il faut couper l'accès à tout élément à examiner pour empêcher toute modification des systèmes locaux connectés au cloud.
- **Capture de l'état de connexion** : Cette coupure permet de récupérer le dernier état de connexion du système avant qu'il ne change.
- **Utilisation d'une cage de Faraday** : Pour les appareils mobiles, cela implique de désactiver physiquement le Wi-Fi ou les connexions cellulaires pour isoler l'appareil du cloud.

4. Moyens de visibilité et outils

Si l'accès direct au serveur cloud est impossible, l'enquêteur peut s'appuyer sur des technologies de sécurité existantes dans l'environnement du client :

- **Pare-feu virtualisés et IPS** : Ces outils déployés dans le cloud génèrent des journaux et des données exploitables.
- **Courtiers de sécurité d'accès au cloud (CASB)** : Un CASB (comme Cisco CloudLock) agit comme un gardien entre l'infrastructure locale et le fournisseur de cloud, offrant une visibilité sur les accès des utilisateurs et les comportements inhabituels.
- **Agents cloud** : Certains agents peuvent être déployés pour collecter du trafic NetFlow ou des fichiers pertinents au sein de l'environnement cloud.

En conclusion, il est essentiel de **consigner rigoureusement l'utilisation du cloud** par chaque ressource dans votre chaîne de traçabilité et vos outils de gestion forensique avant de commencer l'investigation proprement dite.

Comment obtenir un mandat ?

L'obtention d'un mandat est une procédure juridique complexe qui nécessite une collaboration étroite entre l'équipe technique et les experts juridiques pour garantir l'admissibilité des preuves. Selon les sources, voici les étapes et éléments clés pour obtenir et gérer un mandat :

1. Établir la « cause probable »

La plupart des systèmes judiciaires exigent une **cause probable** pour délivrer un mandat. Pour qu'elle soit solide, vous devez :

- Privilégier les **faits incontestables** aux arguments facilement contestables.
- Éviter de vous baser uniquement sur une adresse IP, car celle-ci peut provenir d'un réseau non sécurisé accessible par des tiers, ce qui est souvent jugé insuffisant par un juge.
- Fournir des preuves tangibles et détaillées dans le formulaire de demande pour contrer les contestations de la partie adverse.

2. Collaborer avec une équipe juridique

Il est fortement recommandé de ne pas effectuer la demande seul. Vous devez **travailler avec des juristes** ou un service juridique pour :

- Effectuer la demande en votre nom.
- Confirmer le **nombre d'éléments de preuve** pouvant être soumis (par exemple, le laboratoire de Philadelphie limite souvent à cinq éléments par demande).
- Définir les types d'éléments acceptables, la **durée de l'accès** autorisée et l'étendue exacte des données auxquelles le mandat donne accès.

3. Préparer la demande (Questions clés)

La personne remplissant le formulaire doit être prête à répondre à des questions précises, notamment :

- Qui fait l'objet de l'enquête et quels sont les faits de l'affaire ?
- Quels sont les **éléments d'intérêt** et où se trouvent-ils précisément ?
- Ces éléments peuvent-ils être retirés sans nuire aux personnes ou à l'entreprise ?
- Existe-t-il un stockage de données hors site ou une utilisation du **cloud** ?

- Quelles sont vos qualifications et votre expérience en matière de criminalistique ?

4. Respecter l'étendue et la géographie

Un mandat a des limites strictes que l'enquêteur doit scrupuleusement respecter :

- **Zone géographique** : Vous devez travailler uniquement dans la zone exacte spécifiée (par exemple, une pièce précise ou l'ensemble d'une entreprise).
- **Nouveau mandat** : Si vous découvrez des preuves d'un crime différent de celui visé initialement (par exemple, des images illégales lors d'une enquête pour fraude), un **nouveau mandat** est généralement nécessaire pour étendre la recherche à ces nouvelles preuves.

5. Utiliser des modèles officiels

Pour vous guider, vous pouvez consulter des modèles de formulaires en ligne, comme ceux du **RCFL** (Regional Computer Forensics Laboratory) pour le district du Kansas ou de Philadelphie. L'utilisation de termes juridiques précis est essentielle, car une formulation incorrecte peut invalider l'intégralité de l'enquête.

Enfin, n'oubliez pas que dans de nombreuses entreprises, les employés renoncent à leur droit à la vie privée pour les biens appartenant à l'employeur via des **accords d'utilisation**, ce qui peut parfois permettre un accès sans mandat, bien qu'une consultation juridique reste toujours préférable avant toute action.

Comment faire un hachage ?

Le hachage est une étape technique cruciale pour garantir l'intégrité des preuves numériques. Bien que les sources ne détaillent pas le fonctionnement mathématique de l'algorithme, elles précisent la procédure rigoureuse à suivre pour effectuer et valider un hachage dans un contexte d'enquête.

Voici les étapes et principes de mise en œuvre :

1. Moment de l'exécution

Le hachage doit intervenir immédiatement après la création des copies numériques de l'élément original. Il s'agit de l'une des trois étapes obligatoires avant tout examen :

- Créer plusieurs copies.
- **Valider le hachage** de ces copies.
- Activer la protection en écriture.

2. Outils utilisés

Les sources mentionnent plusieurs outils et environnements permettant de réaliser ou de valider des hachages :

- **Logiciels forensiques** : WinHex, Guidance EnCase 7.12 et les outils natifs de **Kali Linux**.
- **Frameworks d'analyse** : Le *Digital Forensic Framework* (DFF) est cité pour la préparation et la création de copies dont les hachages sont ensuite répertoriés.

3. Documentation et stockage des valeurs

Une fois le hachage calculé, la valeur obtenue doit être traitée avec soin :

- **Rapport d'expertise** : Les valeurs de hachage de chaque copie doivent être consignées dans la section « Acquisition et préparation de l'examen » du rapport.
- **Sécurisation des valeurs** : Ces valeurs doivent être répertoriées et stockées sur un **système d'investigation isolé** pour éviter toute altération ultérieure.

4. Importance de la validation

La validation du hachage sert à démontrer techniquement que les copies sont strictement identiques à l'original. Si vous effectuez une validation avant et après une action (comme un redémarrage) et que vous constatez une modification de la valeur de hachage, cela constitue une **contamination** de la preuve, ce qui peut entraîner le rejet de l'affaire par un tribunal.

En résumé, faire un hachage consiste à utiliser un outil spécialisé pour générer une empreinte numérique unique de la copie, à la comparer à l'original (ou à d'autres copies) pour en confirmer l'exactitude, puis à documenter scrupuleusement ce résultat dans le dossier d'enquête.

Comment organiser le journal ?

L'organisation du journal est une étape cruciale pour assurer la cohérence de l'enquête et éviter que la masse de données recueillies ne devienne chaotique. Selon les sources, voici les meilleures pratiques pour structurer votre journalisation :

1. Utilisation de supports mixtes

Il est recommandé de combiner deux types de journaux pour une flexibilité maximale :

- **Journal papier** : Idéal pour prendre des notes rapides, dessiner des croquis de la scène de crime ou noter des informations verbales via un enregistreur vocal sans attendre le démarrage d'un ordinateur.
- **Journal numérique** : Privilégiez un **logiciel de gestion de cas** (comme Autopsy, DFF ou EnCase) qui guide l'enquêteur, automatise la documentation et facilite la génération de rapports professionnels.

2. Structure hiérarchique (Relation Parent/Enfant)

L'organisation doit suivre une logique de **relation parent/enfant** pour maintenir la traçabilité des preuves.

- Chaque nouvel élément extrait ou découvert est considéré comme un « **enfant** » de l'**élément parent** dont il provient.
- **Dossiers dédiés** : Conservez les éléments provenant d'un appareil spécifique (par exemple, un ordinateur portable) dans un dossier unique pour éviter toute confusion avec d'autres périphériques.
- **Sous-dossiers spécialisés** : Si vous extrayez des données de la RAM, créez un sous-dossier spécifique au sein du dossier de l'hôte pour regrouper ces fichiers.

3. Utilisation d'un séquenceur d'événements

Le journal numérique doit fonctionner comme une **chronologie active** de l'analyse :

- **Séquenceur d'événements** : Utilisez cet outil pour enregistrer chaque découverte (ex: historique de navigation, fichiers récupérés) avec la **date, l'heure précise et une note descriptive**.
- **Validation** : Chaque entrée doit impérativement être **horodatée et validée** par l'enquêteur pour être juridiquement recevable.

- **Traces réseau** : Pour les enquêtes réseau, organisez les résultats par segments, puis par sous-dossiers pour chaque appareil, en y stockant les journaux, les captures de paquets et les tables de routage correspondants.

4. Contenu des notes

Pour que les données soient pertinentes pour le rapport d'expertise, vos notes doivent inclure :

- Les **hypothèses et détails** obtenus lors des entretiens, en étiquetant chaque information avec le nom de la personne qui l'a fournie.
- Des **photographies, vidéos et captures d'écran** de l'état initial des systèmes avant toute interaction.
- Un registre de **chaîne de possession** documentant qui a accès à l'artefact, où il est stocké et son état à chaque étape.

En résumé, une organisation rigoureuse dès le départ, basée sur une **hiérarchie claire et une journalisation chronologique systématique**, protège l'enquêteur contre les contestations de la partie adverse qui pourrait tenter de discréditer des preuves présentées comme incomplètes ou mal documentées.

Quels détails mettre dans le rapport final ?

Le rapport d'expertise est considéré comme la partie la plus visible et l'une des plus importantes d'une enquête médico-légale. Il doit être rédigé de manière à être compris par des publics variés, tels que des gestionnaires, des avocats ou des juges, qui n'ont pas nécessairement d'expertise technique.

Selon les sources, un rapport professionnel doit inclure au minimum les sections suivantes :

1. Résumé de l'affaire

Cette section doit être un **résumé concis** expliquant les raisons de l'implication de l'enquêteur et la nature des preuves numériques analysées. Elle ne doit pas inclure les résultats de l'enquête ni les détails du fond de l'affaire, mais simplement poser le cadre de l'examen.

2. Acquisition et préparation de l'examen

Cette partie détaille toute l'interaction technique avec les preuves pour garantir l'absence de contamination. On doit y trouver :

- Les étapes de la **chaîne de possession** depuis la prise en charge initiale.
- Les **valeurs de hachage** de chaque copie réalisée.
- Les outils logiciels et matériels utilisés (ex : bloqueurs d'écriture).
- Les photographies et notes prises lors de l'acquisition.

3. Constatations (*Findings*)

C'est généralement la section la plus longue car elle décrit les actions menées et les résultats obtenus. Elle doit :

- Mettre en évidence chaque élément de preuve trouvé.
- Expliquer la **méthode employée** pour trouver chaque élément (ex: extraction de registre, historique de navigation).
- Utiliser des hyperliens vers des images ou des annexes pour faciliter la lecture.

4. Conclusion

Elle résume les conclusions basées strictement sur les preuves recueillies. Elle doit :

- Se concentrer exclusivement sur les **faits** et éviter les suppositions non étayées.
- Démontrer que les constatations sont **reproductibles**.
- Éviter les sentiments ou convictions personnelles pour laisser les preuves parler d'elles-mêmes.

5. Liste des auteurs

Cette section identifie toutes les personnes ayant contribué à l'enquête et inclut :

- Leurs **coordonnées complètes**.
- Une section de **signatures** pour authentifier le rapport.
- Une brève **biographie des enquêteurs** pour démontrer leur expertise technique.

Sections optionnelles et bonnes pratiques

Vous pouvez également enrichir le rapport avec une page de titre, une table des matières, un **glossaire des termes techniques** (pour expliquer des acronymes ou des concepts comme les « kits d'exploitation ») et une chronologie détaillée de l'enquête. Enfin, il est fortement recommandé de joindre en annexe les données exportées de

vos outils de journalisation (comme Autopsy) pour prouver la rigueur de votre processus.

Quels logiciels payants choisir à part Autopsy ?

Bien que les sources privilégient **Autopsy** pour sa gratuité et sa disponibilité sous Kali Linux, elles recommandent plusieurs options commerciales (payantes) pour un usage professionnel, car ces logiciels offrent souvent davantage d'options d'enregistrement des artefacts et de meilleures capacités d'exportation de données.

Voici les principaux logiciels payants ou professionnels cités :

- **EnCase (Guidance Software)** : C'est l'une des options les plus populaires recommandées pour la gestion de cas et l'analyse forensique approfondie.
- **X-Ways Forensics** : Une suite logicielle robuste citée comme une alternative efficace pour les enquêtes professionnelles.
- **WinHex** : Utilisé spécifiquement pour l'examen technique et l'analyse des copies de disques par hachage.
- **Digital Forensic Framework (DFF)** : Bien qu'il existe en version libre, il est classé parmi les outils professionnels performants pour la préparation et l'examen des preuves.
- **Eraser** : Un logiciel professionnel de suppression de données qui offre une interface graphique conviviale pour effacer définitivement des fichiers au niveau forensique.
- **TimeLive** : Recommandé pour compléter les logiciels d'analyse, car il permet de gérer la **facturation** et le suivi des heures de travail des enquêteurs, des fonctionnalités qu'Autopsy ne propose pas.

Les sources soulignent qu'un **logiciel de gestion de cas d'entreprise** est souvent préférable à Autopsy pour un usage professionnel, car ce dernier présente certaines lacunes, notamment en ce qui concerne l'exportation des données pour les rapports finaux. Il est conseillé de tester plusieurs de ces outils pour déterminer celui qui correspond le mieux à votre style d'enquête.

Comment prouver la cause probable ?

Pour prouver la **cause probable** (*probable cause*) lors de la demande d'un mandat, les sources recommandent une approche rigoureuse basée sur des faits vérifiables et une collaboration étroite avec des experts juridiques.

Principes fondamentaux pour établir la cause probable

- **Privilégier les faits incontestables** : Il est fortement conseillé de s'appuyer sur des faits concrets et solides plutôt que sur des arguments facilement contestables par la partie adverse.
- **Éviter les preuves insuffisantes** : Par exemple, fonder une cause probable uniquement sur une **adresse IP** liée à un domicile est souvent jugé insuffisant. Un juge peut considérer que n'importe qui aurait pu accéder à un réseau sans fil non sécurisé à cet endroit pour commettre l'infraction.
- **Fournir des preuves tangibles** : La demande doit inclure des preuves détaillées et tangibles pour contrer les contestations potentielles du juge ou des avocats de la partie adverse.

Éléments à inclure dans la démonstration

La personne qui remplit la demande doit être prête à étayer sa cause probable en répondant à des questions précises dans le formulaire de mandat, notamment :

- Les **faits précis** de l'affaire.
- L'identification claire de la personne faisant l'objet de l'enquête.
- La description des **éléments d'intérêt** et leur localisation exacte.
- Une explication de ce que l'enquêteur **pense trouver** et pourquoi ces éléments constituent une preuve.

Importance de la terminologie

Le choix des mots est déterminant pour convaincre un tribunal de la validité de la cause probable. Les sources notent que certains termes ont une portée juridique plus forte que d'autres :

- La mention de « **pédopornographie** » sera plus déterminante pour obtenir un mandat que celle de « comportement à caractère sexuel explicite », car elle relève de lois prévoyant des peines sévères plutôt que d'une simple violation du règlement intérieur d'une entreprise.

Enfin, il est recommandé d'organiser une réunion avec une **équipe juridique** pour confirmer ces détails techniques et s'assurer que la formulation utilisée ne risque pas d'invalidier l'ensemble de l'enquête