Récupération de données

Manuel de référence — Édition mai 2026

Par Mhessan Kouassi
Expert en récupération de données chez DAFOTEC

Laboratoire DAFOTEC • Roubaix • Salle blanche ISO 5 • Depuis 2004

Anatomie des supports, méthodes professionnelles, outils ouverts et commerciaux, prévention. Toutes les affirmations chiffrées sont sourcées ou explicitement qualifiées d'ordres de grandeur. Aucun cas n'est inventé : les incidents historiques cités sont publics et référencés, les retours de laboratoire DAFOTEC sont issus de cas réels anonymisés publiés sur dafotec.fr.

Document de référence pour techniciens, étudiants en forensique, particuliers avancés et décideurs informatiques.

Préface

Pourquoi ce manuel existe — et contre quoi il réagit

J'exerce le métier de récupérateur de données depuis 2004. Dans le laboratoire DAFOTEC à Roubaix, j'ai ouvert, diagnostiqué et imagé plus de 120 000 supports — disques durs claqués, SSD mutiques, RAID dégradés après surtension, smartphones écrasés, NAS chiffrés par ransomware. Cette pratique, accumulée sur 22 ans, m'a appris une chose simple : **en récupération de données, la première mauvaise décision est presque toujours plus coûteuse que la panne elle-même**.

Ce manuel n'a pas été écrit pour promettre une récupération partout ; il a été écrit pour éviter les erreurs qui rendent la récupération impossible. C'est une distinction qui paraît modeste, mais elle dessine en creux toute la discipline. Quand un client arrive au laboratoire avec un disque qui claque et qu'il a déjà fait tourner trois logiciels « pour voir », nous n'avons plus le même problème à traiter qu'au début de l'incident. Quand un DSI relance une reconstruction RAID sur un array dégradé sans imager d'abord, l'écart entre ce qui était récupérable et ce qui l'est encore se mesure parfois en années d'archives.

Le secteur souffre d'une désinformation chronique. Des logiciels grand public promettent de récupérer « 100 % » des fichiers sur n'importe quel support. Des tutoriels YouTube recommandent le congélateur pour les disques durs et le riz pour les téléphones tombés à l'eau. Des comparatifs en ligne annoncent des taux de succès chiffrés à la virgule sans la moindre méthodologie publique. Ce manuel se construit explicitement contre cette littérature : chaque chiffre est sourcé ou présenté comme un ordre de grandeur, chaque méthode est documentée avec ses limites, chaque promesse est qualifiée par ce qu'elle suppose.

L'autre raison de ce manuel est plus pratique. Les supports modernes — SSD avec TRIM agressif, Mac avec Secure Enclave, NAS chiffrés par ransomware, RAID en SMR — ont rendu obsolète une partie des réflexes hérités de l'âge d'or des disques magnétiques. Sur un HDD des années 2000, on avait des jours voire des semaines pour récupérer un fichier supprimé. Sur un SSD NVMe moderne en bonne santé, la fenêtre se mesure parfois en secondes après le TRIM. La discipline a changé ; les réflexes doivent suivre.

Je distille ici quatre principes qui résument 22 ans de métier :

- **L'expérience de terrain montre qu'une mauvaise tentative bien intentionnée détruit plus de données qu'une panne logique simple.**
- **En récupération de données, les dix premières minutes décident souvent des dix prochaines années d'archives d'une entreprise.**
- **Chez DAFOTEC, le diagnostic précède toujours l'outil : on ne lance pas un scan pour voir, on qualifie d'abord le risque.**
- **Le rôle d'un professionnel sérieux n'est pas de promettre un miracle, mais de dire honnêtement ce qui est encore récupérable, ce qui ne l'est plus, et ce qu'il ne faut surtout pas faire ensuite.**

Bonne lecture. Et bonnes sauvegardes.

Mhessan Kouassi
Expert en récupération de données • DAFOTEC, Roubaix
Mai 2026

Avertissement et méthode

Trois règles ont gouverné l'écriture de ce manuel :

- Chaque pourcentage est sourcé ou explicitement étiqueté comme ordre de grandeur quand aucune statistique publique ne le justifie.
- Aucun cas n'est inventé. Les incidents historiques cités (NotPetya/Maersk 2017, Code Spaces 2014) sont publics et référencés. Les « retours de labo DAFOTEC » sont des interventions réelles, anonymisées, publiées par DAFOTEC sur dafotec.fr.
- Les méthodes propriétaires DAFOTEC mentionnées dans le texte — VeriFiles, SEAD, greffe HSA, Spider Web, Reverse FTL, CPU Swap — sont documentées sur le site officiel ; ce manuel les présente dans leur contexte technique.

À qui s'adresse ce livre

Aux techniciens IT qui doivent gérer des incidents de perte de données ; aux étudiants en forensique numérique qui cherchent une vue d'ensemble pédagogique ; aux particuliers avancés qui veulent comprendre ce qui se passe sous le capot avant d'agir ou de confier leur support à un laboratoire ; aux juristes et experts judiciaires qui ont besoin d'une vue technique pour évaluer la recevabilité d'éléments numériques ; aux dirigeants et DSI qui veulent évaluer leur posture de prévention.

À qui il ne s'adresse pas

À quelqu'un qui a une urgence active et n'a pas le temps de lire. Dans ce cas, la règle est simple : **débrancher le support, ne rien y écrire, et soit consulter le chapitre 5 (diagnostic) pour se positionner, soit contacter directement un laboratoire**. Le diagnostic est gratuit chez DAFOTEC ; vous pouvez donc obtenir un avis professionnel avant toute décision financière.

Avertissement légal

La récupération de données sur des supports qui ne vous appartiennent pas, ou qui contiennent des données protégées par le secret professionnel ou le RGPD, est encadrée par la loi. Les techniques décrites ici sont à usage éducatif et professionnel uniquement. Pour tout enjeu sérieux — données médicales, judiciaires, propriété intellectuelle — passer par un laboratoire sous contrat de confidentialité reste la seule voie acceptable. DAFOTEC opère sous accord de confidentialité (NDA) systématique pour les supports professionnels, en conformité RGPD et ISO 27001.

Sommaire

INTRODUCTION

Chapitre 0

La récupération de données en 2026

Une discipline à l'intersection de plusieurs métiers

La récupération de données est l'ensemble des techniques permettant de retrouver des informations rendues inaccessibles sur un support de stockage. La discipline mobilise quatre familles de compétences : physique des matériaux (magnétisme pour les disques durs, électronique à grille flottante ou piégeage de charge pour les mémoires NAND), algorithmique des systèmes de fichiers, ingénierie inverse de contrôleurs propriétaires, et rigueur procédurale forensique.

On la distingue soigneusement de la **restauration de sauvegarde**, qui relève de la prévention. La récupération intervient après la perte, sur un support qui n'a pas de copie utilisable. C'est, par construction, une discipline d'urgence où l'on fait avec ce qu'il reste.

Deux mondes, jamais à confondre

Récupération logique : le support est physiquement intact et détecté par la machine. Le problème est dans le logiciel — système de fichiers corrompu, partition supprimée, fichiers effacés, chiffrement par ransomware. Les données brutes sont presque toujours encore là ; il faut juste savoir les lire.

Récupération physique : panne matérielle. Le support n'est plus détecté, ou émet des bruits anormaux, ou son contrôleur ne répond plus. L'intervention demande un environnement spécialisé : salle blanche pour les disques durs mécaniques, station de micro-soudure pour les SSD.

Tout le travail de récupération commence par un diagnostic qui tranche entre ces deux mondes. Se tromper de monde coûte des données. Le chapitre 5 détaille cette étape.

L'évolution depuis 1990

Pendant trois décennies, la récupération s'est faite sur disques durs magnétiques. Le principe était stable : tant que les plateaux n'étaient pas physiquement réécrits, les données restaient en place. Suppression, formatage rapide, corruption logique : tout cela n'affectait que la table d'allocation, pas le contenu. C'était l'âge d'or des logiciels grand public type Norton Utilities ou, plus tard, TestDisk.

L'arrivée massive des SSD à partir de 2010 a fait basculer la discipline. La mémoire NAND ne se comporte pas comme un disque magnétique : on ne peut pas réécrire en place, et le contrôleur doit en permanence consolider et effacer des blocs entiers. Avec la commande **TRIM** (apparue dans Windows 7, macOS 10.6.8 et le noyau Linux 2.6.33), supprimer un fichier déclenche un effacement *physique* des cellules concernées, souvent en quelques secondes à minutes. Sur SSD moderne en bonne santé, la fenêtre de récupération logique se réduit dramatiquement.

Parallèlement, deux autres évolutions ont remodelé le paysage : la généralisation du **chiffrement matériel** (SED, TCG Opal, BitLocker avec TPM, FileVault avec Secure Enclave) qui rend la donnée physique inutilisable sans la clé, et l'explosion des attaques par **ransomware** qui ciblent désormais explicitement les sauvegardes. Le Verizon DBIR 2025 chiffre cette dernière tendance : le ransomware est impliqué dans 44 % des compromissions de données documentées en 2024, en hausse de 37 % sur un an.

Sur les statistiques — Aucune statistique consolidée publique ne donne le taux de réussite global de la récupération de données. Les laboratoires professionnels publient parfois des chiffres dans leurs supports commerciaux. DAFOTEC publie publiquement les siens sur dafotec.fr — par type de panne, sur les 120 000+ cas traités depuis 2004 : 95 % sur panne logique HDD, 88 % sur panne électronique HDD, 78 % sur panne mécanique HDD, 82 % sur SSD firmware, 61 % sur SSD panne NAND, 91 % sur RAID 5 dégradé, 69 % sur smartphone. Ces chiffres ne valent que pour DAFOTEC et pour des supports non aggravés par des tentatives préalables.

Comment ce livre est organisé

Sept parties, dix-neuf chapitres et quatre annexes. La progression est délibérée : on commence par comprendre ce qu'est physiquement un support de stockage (partie I), puis comment diagnostiquer une panne (partie II), puis quelles méthodes appliquer (partie III), puis comment gérer les cas particuliers (partie IV), puis quels outils choisir dans la pratique (partie V), puis comment rendre tout cela inutile par une bonne prévention (partie VI), et enfin où va la discipline dans les années qui viennent (partie VII).

Quatre conventions de mise en page :

- Les encadrés **bleus** sont des notes pédagogiques.
- Les encadrés **orange** sont des avertissements opérationnels — à lire avant d'agir.
- Les encadrés **verts** sont des études de cas publiques et sourcées (incidents historiques publiquement documentés).
- Les encadrés **beiges marqués « Retour de labo — DAFOTEC »** sont des interventions réelles, anonymisées, publiées par DAFOTEC sur son site officiel.

Partie I

Fondations physiques

Avant toute méthode, il faut comprendre *physiquement* comment une donnée est écrite, lue et supprimée. Trois chapitres : un disque dur mécanique (HDD), une mémoire NAND (SSD, eMMC, UFS, carte SD), un système de fichiers (la couche logique qui organise les blocs en arborescence). Sans cette base, les méthodes des chapitres suivants ne sont que de la magie.

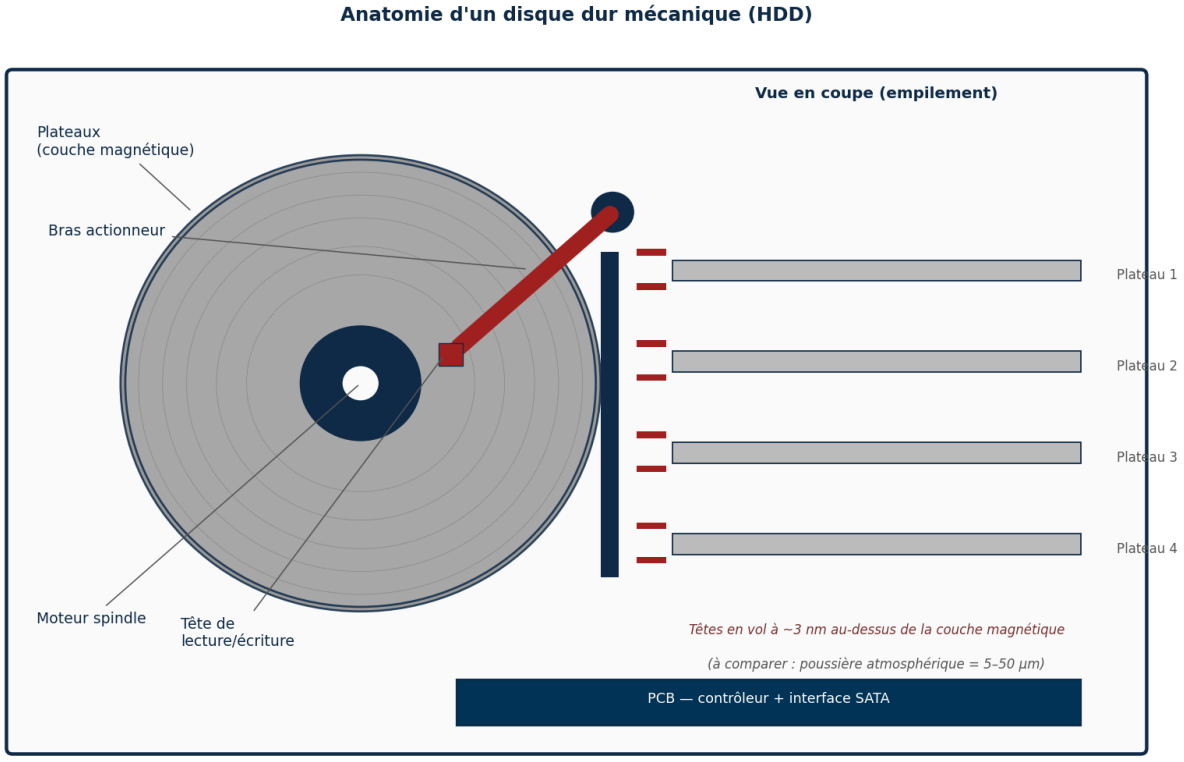
PARTIE I — FONDATIONS PHYSIQUES

Chapitre 1

Anatomie d'un disque dur mécanique

1.1 Vue d'ensemble

Un disque dur (HDD, *Hard Disk Drive*) est une mécanique de précision miniaturisée. Sous son boîtier hermétique, on trouve : un ou plusieurs **plateaux** rigides revêtus d'une couche magnétique, un **moteur spindle** qui les fait tourner à vitesse constante, des **têtes de lecture/écriture** portées par un **bras actionneur** qui balaye la surface, et un **circuit imprimé** (PCB) extérieur qui contient le contrôleur, la ROM de firmware et l'interface SATA ou SAS.



Anatomie schématique d'un HDD 3,5" : plateaux, bras, têtes en vol nanométrique, PCB.

Les ordres de grandeur typiques d'un HDD 3,5" grand public en 2026 :

Paramètre	Valeur typique
Vitesse de rotation	5 400 ou 7 200 tr/min (consumer), jusqu'à 15 000 (enterprise SAS)
Capacité par plateau	2 à 4 To
Nombre de plateaux	1 à 10 selon la capacité totale
Densité linéaire	Plus de 1 million de bits par pouce de piste
Vol des têtes (fly height)	Quelques nanomètres au-dessus du plateau
Débit séquentiel	150 à 300 Mo/s

Paramètre	Valeur typique
Latence d'accès aléatoire	5 à 15 ms

1.2 Comment une donnée est écrite

La couche magnétique du plateau est divisée en milliards de petits domaines magnétiques. La tête d'écriture, en générant un champ magnétique local très fort et très bref, oriente la polarisation d'un domaine dans un sens (bit 1) ou dans l'autre (bit 0). La transition entre deux polarisations opposées est ce que la tête de lecture détecte ensuite, par induction ou plus récemment par effet tunnel magnétorésistif (TMR).

Tant que rien ne réécrit la zone, ces polarisations magnétiques sont **stables sur des décennies**. C'est la propriété fondamentale qui rend les HDD si récupérables : effacer un fichier au niveau du système de fichiers ne touche pas aux domaines magnétiques eux-mêmes.

1.3 PMR, CMR, SMR, HAMR : les technologies d'écriture

Quatre technologies coexistent ou se succèdent :

- **PMR** (Perpendicular Magnetic Recording) : depuis 2005, les domaines magnétiques sont orientés perpendiculairement à la surface plutôt que parallèlement. C'est la base de tous les HDD modernes.
- **CMR** (Conventional Magnetic Recording) : terme moderne qui désigne le PMR « classique » avec des pistes écrites côte à côte sans recouvrement. Permet de réécrire n'importe quelle piste sans toucher aux voisines.
- **SMR** (Shingled Magnetic Recording) : depuis 2013, les pistes se recouvrent partiellement comme des tuiles de toit. On gagne 20 à 25 % de densité, mais chaque modification d'une piste oblige à réécrire toute la bande de pistes adjacentes. Le firmware doit gérer une zone de cache et un garbage collection comparable à celui d'un SSD.
- **HAMR** (Heat-Assisted Magnetic Recording) : technologie qui chauffe ponctuellement le domaine par laser pendant l'écriture pour réduire la taille des domaines stables. Commercialisée à partir de 2024 sur les disques entreprise très haute capacité (30 To+).

SMR et récupération — Le SMR est sensiblement plus complexe à récupérer en cas de panne firmware : la translation entre adresses logiques (LBA) et emplacements physiques sur la bande est gérée par le contrôleur, et un firmware corrompu peut rendre le contenu illisible même sur des plateaux intacts. Les laboratoires utilisent des modules spécialisés (PC-3000 a publié des modules SMR à partir de 2020) qui doivent gérer à la fois le translator principal et le cache translator. Source : Rossmann Group, *CMR vs SMR: How Recording Technology Affects Recovery*, 2026.

1.4 Causes typiques de panne mécanique

1. **Head crash.** Une tête entre en contact avec la surface du plateau — choc, vibration, défaut de fly height. Le résultat est souvent une rayure progressive qui détruit physiquement la couche magnétique. Symptôme classique : *clics répétés* de la tête qui cherche en vain à se positionner.
2. **Stiction.** Les têtes restent collées au plateau au lieu de se parquer correctement à l'arrêt. Le moteur n'arrive plus à lancer la rotation. Symptôme : *bruit de bourdonnement court puis silence*.

3. **Moteur spindle HS.** Les paliers s'usent, le moteur grippe. Symptôme : *plateau qui ne tourne plus du tout, ou tourne par à-coups*.
4. **PCB grillé.** Une surtension détruit des composants du circuit imprimé, souvent le TVS (transistor de protection). Le disque n'est plus détecté du tout, parfois il fume littéralement.
5. **Corruption firmware.** La ROM du PCB ou une zone système des plateaux (zone de service, détaillée plus bas) devient illisible. Le disque tourne mais ne se monte pas, ou se monte avec une capacité absurde (0 Go, 8 Mo, valeur incohérente).

Attention — Un HDD qui claque doit être éteint immédiatement. Chaque rotation supplémentaire des plateaux quand les têtes touchent la surface étend la zone rayée — chaque seconde, on perd des données. C'est l'une des rares vraies urgences en récupération.

1.5 Pourquoi un HDD reste très récupérable

Quand un système de fichiers supprime un fichier, il modifie seulement ses propres tables internes (MFT pour NTFS, inodes pour ext4, table FAT pour FAT32/exFAT). Les secteurs physiques qui contenaient le fichier ne sont ni effacés, ni démagnétisés. Ils le seront seulement quand un nouveau fichier viendra écrire par-dessus.

C'est pour cela que sur un HDD :

- Un fichier supprimé est récupérable tant que ses secteurs n'ont pas été réutilisés.
- Un formatage rapide ne fait que réinitialiser les structures de base du FS ; les secteurs restent intacts.
- Un formatage complet (qui réécrit tout) détruit effectivement les données, mais prend des heures et n'est presque jamais fait par accident.

Sur un HDD non écrasé, les outils de récupération logique (TestDisk, R-Studio, UFS Explorer, PhotoRec en dernier recours) retrouvent en pratique l'écrasante majorité des données.

1.6 La fiabilité moyenne d'un HDD en 2026

Backblaze, hébergeur cloud, publie depuis 2013 les statistiques de panne de son parc de disques durs. Le rapport annuel 2025 (publié en février 2026) compte 344 196 disques répartis sur 30 modèles. Trois chiffres clés :

- AFR annuel 2025 : **1,36 %** (en baisse par rapport à 1,55 % en 2024).
- AFR sur la vie complète des disques (lifetime) : **1,30 %**, stable d'un trimestre à l'autre.
- Q4 2025 a affiché un AFR trimestriel de 1,13 %, le plus bas depuis 2022.

Autrement dit : sur un échantillon massif, environ 1,4 % des disques tombent en panne chaque année. Pour un particulier qui a un seul disque, cela ne dit pas grand-chose individuellement — votre disque personnel tombera en panne ou non, c'est binaire. Mais cela rappelle que sur un parc, la panne est statistiquement certaine.

Source : Backblaze, Drive Stats for 2025, rapport annuel publié le 12 février 2026.

1.7 Zone de service, modules firmware, translator

Une part cruciale de l'intelligence d'un HDD ne se trouve ni sur le PCB ni dans le contrôleur, mais dans une zone particulière des plateaux eux-mêmes : la **Service Area** (SA, zone de service), invisible pour le système d'exploitation. Elle contient plus d'une centaine de modules de firmware indispensables au fonctionnement du disque. Trois familles méritent d'être nommées :

- **P-List** (Primary defect list, module 0A sur WD ROYL). Liste des secteurs défectueux identifiés *en usine*, à la sortie de la chaîne de fabrication. Ces secteurs sont remappés dès le départ et ne sont jamais accessibles via les LBA.
- **G-List** (Grown defect list, module 0B). Secteurs qui sont devenus défectueux *pendant la vie* du disque et que le firmware a réalloués automatiquement vers des secteurs de réserve.
- **Translator** (module 028 sur WD ROYL, équivalents sur Seagate, Toshiba, etc.). Module central qui traduit les adresses logiques (LBA) exposées au système en adresses physiques sur les plateaux (cylindre, tête, secteur). Sa corruption rend un disque parfaitement mécaniquement sain *totalement illisible* par l'OS.
- **Adaptives** (modules 102 à 109 sur WD). Paramètres de calibration des têtes, spécifiques à chaque exemplaire de disque, ajustés à la fabrication. C'est ce qui rend impossible un simple PCB swap : il faut transférer ces paramètres.

Sur un disque SMR, le translator est encore plus critique : il doit aussi gérer le mapping entre les zones de cache CMR et les bandes shingled. Une coupure d'alimentation brutale pendant une opération de garbage collection peut corrompre ce mapping et rendre des téraoctets de données inadressables. La récupération consiste alors à **reconstruire ou réparer le translator** à l'aide d'outils spécialisés type PC-3000 — en pratique, c'est ce qui se fait quotidiennement dans les laboratoires équipés. Sources : ACE Lab (documentation publique PC-3000), Rossmann Group, ISA Group *HDD Service Area Modules Reference*.

Diagnostiquer une panne SA — Symptôme typique d'une corruption de Service Area : le disque est détecté par le BIOS mais affiche une capacité absurde (0 Go, 8 Mo, valeur cohérente mais fausse), ou est détecté sous un nom générique du fabricant. Le disque tourne normalement, n'émet aucun bruit anormal — c'est uniquement logique côté firmware interne. Diagnostic réservé au laboratoire : le terminal série TTL sur le PCB est nécessaire pour accéder à la SA.

RETOUR DE LABO — DAFOTEC • Disque dur WD Blue 2 To, têtes HS (cas n°1)

Support : WD Blue 2 To 3,5" • **Délai :** 72 heures • **Forfait :** 650 € HT

Symptôme. Clics répétés toutes les 3 secondes, disque non détecté, après une chute de 80 cm sur carrelage du boîtier externe.

Intervention. Ouverture en salle blanche ISO 5, remplacement du bloc de têtes (HSA) par un disque donneur identique de même révision firmware, avec alignement micrométrique inférieur à 0,3 µm. Clonage secteur par secteur avec timeout réduit pour ménager la nouvelle combinaison têtes/plateaux.

Résultat. 1,94 To récupérés sur 2 To. 3 vidéos 4K partiellement corrompues n'ont pu être restaurées intégralement à cause d'une zone de plateau légèrement rayée par la chute.

Photographe professionnel, Paris — 4 ans d'archives sauvées. Cas publié sur dafotec.fr.

PARTIE I — FONDATIONS PHYSIQUES

Chapitre 2

Anatomie d'un SSD : NAND, contrôleur, FTL

2.1 Un changement de paradigme

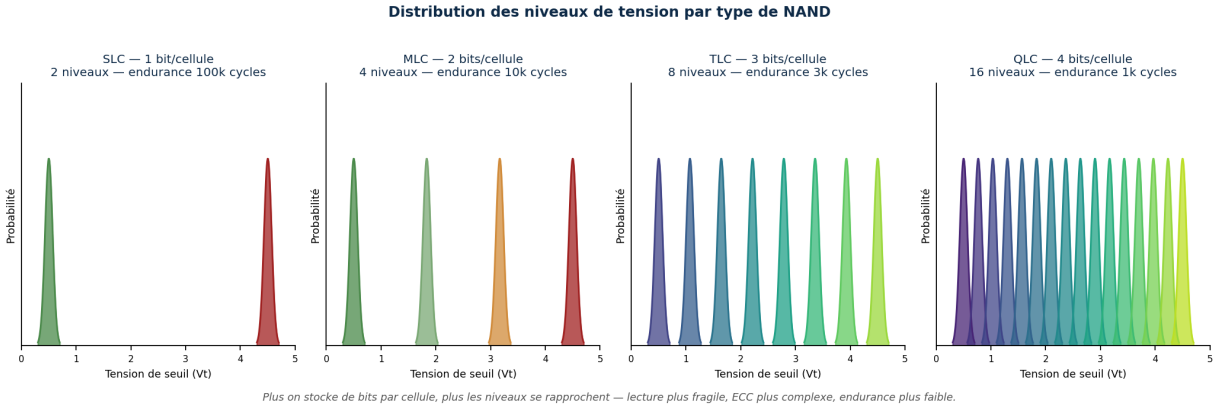
Un SSD (*Solid State Drive*) n'a pas de pièces mécaniques. Toute la complexité est dans l'électronique. Cela paraît une simplification, mais pour la récupération, c'est l'inverse : la mémoire NAND impose des contraintes physiques qui forcent le contrôleur à effacer activement les données supprimées. Sur un HDD, supprimer ne détruit rien ; sur un SSD moderne, supprimer *détruit* dans les minutes qui suivent.

2.2 Les cellules NAND : floating-gate et charge-trap

L'unité fondamentale est la cellule NAND. Historiquement, c'était un transistor à **grille flottante** (floating-gate MOSFET) : une charge électrique piégée entre deux couches isolantes modifie la tension de seuil du transistor. En mesurant cette tension, on lit la valeur stockée.

Depuis les générations 3D NAND (2013 puis massivement à partir de 2017), la technologie a basculé vers le **charge-trap flash** (CTF). Au lieu d'une grille conductrice, on utilise un isolant qui piège les électrons. Avantages : meilleure résistance à l'usure, fabrication plus simple en 3D, moins de fuites entre cellules voisines. La quasi-totalité des SSD grand public 2026 (176 à 232 couches BiCS6, V8 Samsung, etc.) utilisent du charge-trap.

Selon le nombre de niveaux de tension qu'on distingue dans une même cellule, on stocke plus ou moins de bits. C'est le cœur du trade-off densité / endurance / fiabilité :



Plus on stocke de bits par cellule, plus les niveaux se rapprochent (SLC : 2 niveaux écartés ; QLC : 16 niveaux séparés par moins de 200 mV).

Type	Bits/cell	Niveaux	Endurance (cycles P/E)	Usage
SLC	1	2	50 000 à 100 000	Industriel, enterprise critique
MLC	2	4	3 000 à 10 000	Enterprise (en voie de disparition)
TLC	3	8	1 000 à 3 000	Consumer SSD courant 2026
QLC	4	16	150 à 1 000	Grande capacité bon marché

Type	Bits/cell	Niveaux	Endurance (cycles P/E)	Usage
PLC	5	32	moins de 150 (estim.)	En développement, peu commercialisé

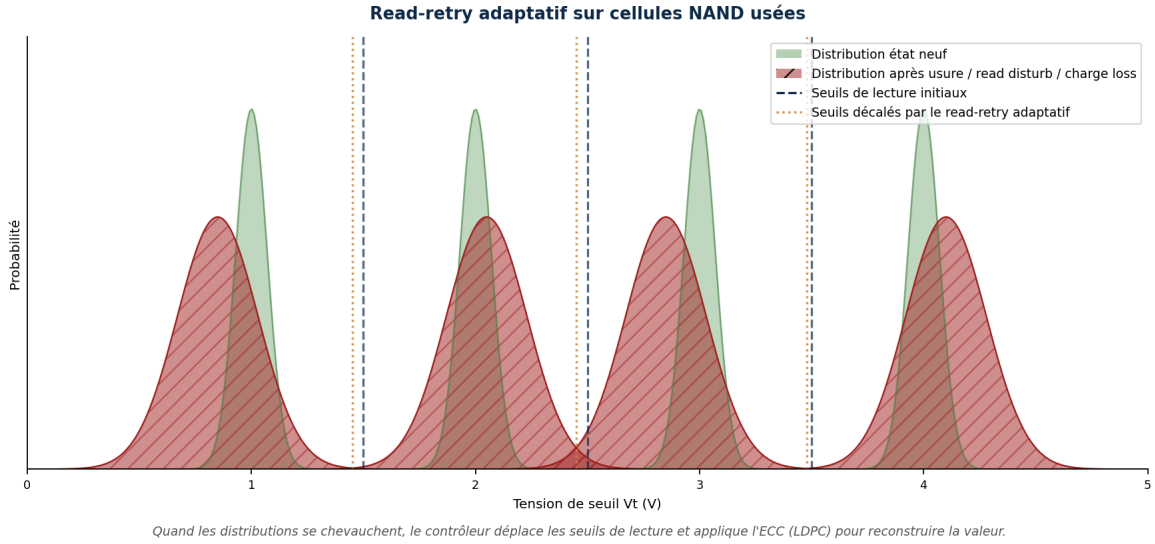
Sources : Kingston Technology, Lexar Enterprise, TechTarget, OSCOO. Les ordres de grandeur d'endurance varient selon les modèles précis ; ces valeurs représentent le haut de la fourchette typique en 2024-2026.

Plus on stocke de bits par cellule, plus la marge entre niveaux est étroite (en QLC, moins de 200 mV entre deux états voisins), plus les erreurs de lecture sont fréquentes, plus le contrôleur doit appliquer de codes correcteurs (ECC), et plus la cellule s'use vite à chaque cycle d'écriture/effacement.

2.3 ECC, LDPC et read-retry adaptatif

À mesure que les marges se sont resserrées, les codes correcteurs ont évolué. Les premiers SSD MLC utilisaient des codes **BCH** (Bose-Chaudhuri-Hocquenghem), simples et déterministes. Les SSD modernes TLC/QLC utilisent presque tous des codes **LDPC** (Low-Density Parity-Check), plus puissants mais plus complexes : le décodeur fonctionne en plusieurs itérations probabilistes.

Quand la lecture brute donne trop d'erreurs pour que l'ECC seul corrige (cellules très usées, perturbation par les lectures voisines, perte de charge dans le temps), le contrôleur déclenche le **read-retry** : il modifie le seuil de tension de référence et relit la même page, parfois cinq, dix ou quinze fois avec des seuils différents. Combinés au décodage LDPC *soft* (qui utilise des informations probabilistes plutôt que binaires), ces retries permettent de récupérer des données que la lecture initiale aurait abandonnées.



Le read-retry décale les seuils pour distinguer des distributions qui se chevauchent après usure ou read disturb.

ECC et chip-off — Pour la récupération par chip-off (chapitre 10), tout cela constitue une difficulté majeure : lire la NAND brute hors de son contrôleur d'origine, c'est obtenir des données *après scrambling et avant décodage ECC*. Il faut savoir reverse engineerer à la fois le scrambler et le pipeline ECC du contrôleur d'origine. C'est l'une des raisons pour lesquelles les laboratoires sérieux (DAFOTEC, ACE Lab clients) maintiennent des bases de profils par contrôleur et par firmware.

2.4 La contrainte fondamentale : écrire à la page, effacer au bloc

C'est **le** détail qui explique tout le reste. La mémoire NAND peut être lue et écrite au niveau de la **page** (typiquement 4, 8 ou 16 Ko), mais elle ne peut être effacée qu'au niveau du **bloc** (256 à 512 pages, soit typiquement 1 à 8 Mo). On ne peut pas réécrire en place : il faut effacer le bloc entier d'abord.

Pour rester performant, le contrôleur ne fait jamais cette opération de manière naïve. Quand on modifie un fichier, il :

1. Écrit la nouvelle version dans une page libre, ailleurs sur la NAND.
2. Met à jour sa table interne de correspondance (**FTL — Flash Translation Layer**) pour que le LBA logique pointe désormais vers la nouvelle page.
3. Marque l'ancienne page comme « invalide » mais ne l'efface pas immédiatement.
4. Plus tard, en arrière-plan, le **garbage collector** consolide les pages valides restantes des blocs partiellement utilisés et applique la tension d'effacement sur les blocs vides.

2.5 Wear leveling, over-provisioning, chiffrement matériel

Comme chaque cellule a une endurance limitée, le contrôleur applique du **wear leveling** : il répartit les écritures sur toutes les cellules disponibles, pour qu'aucune ne s'use plus vite que les autres. Une zone d'**over-provisioning** (7 % minimum, souvent 14 % à 28 % sur les SSD entreprise) est invisible pour l'utilisateur mais utilisable par le contrôleur pour ses opérations de réorganisation et pour remplacer les cellules qui finissent par mourir.

Élément critique souvent ignoré : sur la majorité des SSD modernes (Phison E18, Silicon Motion SM2264, Samsung Pablo, etc.), **tout le contenu de la NAND est chiffré matériellement en AES-256**, même quand l'utilisateur n'a défini aucun mot de passe. La clé maître est dérivée d'un identifiant unique du contrôleur (UID) et stockée dans une zone protégée. Quand le contrôleur meurt, on perd à la fois la table FTL et la clé. Le chip-off donne alors des données chiffrées dont la clé est définitivement perdue.

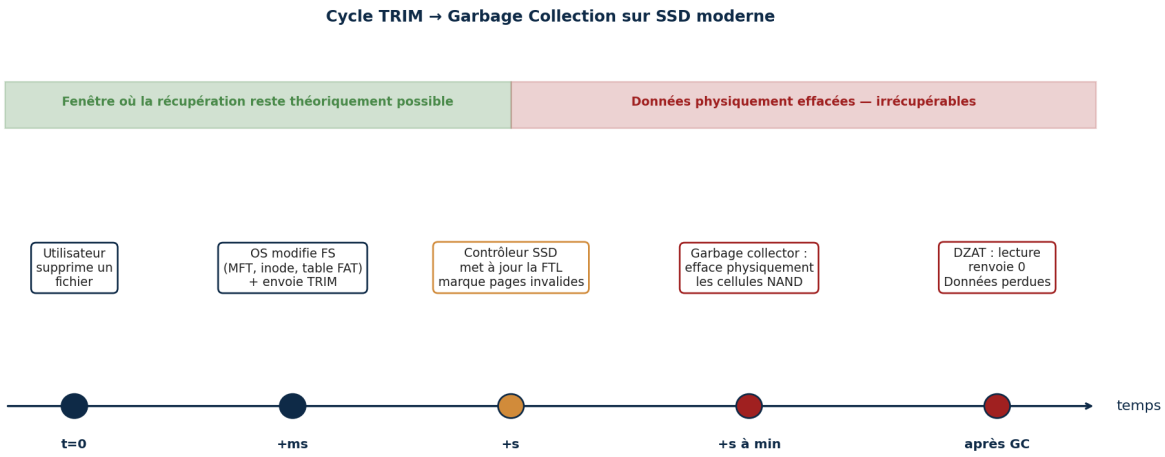
2.6 TRIM : la commande qui change tout

Sans TRIM, le contrôleur n'a aucune idée des pages qui sont encore utilisées au niveau du système de fichiers. Quand l'OS supprime un fichier, il modifie ses propres tables mais ne le dit pas au SSD. Résultat : le contrôleur considère ces pages comme contenant des données valides, et son garbage collector perd un temps fou à les déplacer inutilement.

TRIM (commande ATA DATA SET MANAGEMENT avec l'attribut Trim, ou son équivalent NVMe DEALLOCATE) résout ce problème en informant le contrôleur des LBA libres côté OS. Le contrôleur peut alors :

- Mettre à jour sa table de mapping immédiatement.
- Programmer ces blocs pour effacement physique au prochain cycle de garbage collection.

Sur la plupart des SSD modernes implémentant DRAT (*Deterministic Read After Trim*) ou DZAT (*Deterministic Zero After Trim*), toute lecture ultérieure des LBA trimés renvoie respectivement une valeur déterministe non spécifiée ou des zéros. Les outils de récupération logique ne voient plus rien d'utile.



Cycle TRIM puis garbage collection : la fenêtre de récupération se referme en quelques secondes à minutes.

2.7 La fenêtre de récupération

Combien de temps avant que les données soient physiquement perdues ? Sur SSD NVMe moderne avec TRIM actif :

- À la suppression d'un fichier sur un SSD interne monté en NTFS/APFS/ext4 sous Windows/macOS/Linux récent : TRIM est envoyé immédiatement (millisecondes).
- Le garbage collector peut s'activer dès la prochaine période d'inactivité, donc en quelques secondes à minutes au maximum.
- Une fois le bloc effacé physiquement, aucun chip-off ne récupère quoi que ce soit. Les cellules sont à leur état neutre.

Attention — Si vous avez supprimé un fichier important sur un SSD : **débranchez le support immédiatement**, ne le rebranchez plus sur la même machine, et envoyez-le pour analyse. Chaque seconde sous tension réduit les chances. Et même en agissant vite, considérez que la perte est probable — pas certaine, mais probable.

2.8 Quand TRIM ne fonctionne pas

La récupération SSD reste possible dans plusieurs configurations où TRIM est court-circuité, documentées notamment par Belkasoft (*Recovering Evidence from SSD Drives*, Forensic Focus). Voici les principales :

- **RAID matériel.** La plupart des contrôleurs RAID ne passent pas TRIM aux disques sous-jacents.
- **SSD externes via vieux ponts USB-SATA.** Les JMicron JMS539 et ASMedia ASM1051 anciens ne passent pas TRIM. Les ponts UASP récents (JMS578, ASM235CM, RTL9210B) le passent.
- **NAS.** Selon le firmware et la configuration des volumes, TRIM peut être absent ou différé.
- **Pseudo-SSD bas de gamme.** Certaines clés USB et cartes SD marketées comme SSD n'implémentent pas TRIM.
- **Firmware buggé.** Plusieurs modèles (notamment des Crucial M4, OCZ Vertex, Intel 320) ont eu en sortie d'usine un TRIM cassé.

- **Petits fichiers stockés en interne dans le MFT NTFS.** Les fichiers d'environ 700 octets ou moins sont stockés directement dans l'entrée MFT (attribut $DATA résident) et ne sont jamais affectés par TRIM.
- **Fragments dans des blocs encore partiellement utilisés.** Tant qu'un bloc NAND contient au moins une page valide, il ne peut pas être effacé en entier — les pages invalides du même bloc survivent jusqu'au prochain GC.

2.9 Comment vérifier si TRIM est actif

```
Windows : fsutil behavior query DisableDeleteNotify
(DisableDeleteNotify=0 -> TRIM activé,
DisableDeleteNotify=1 -> TRIM désactivé)

Linux : cat /sys/block/sdX/queue/discard_max_bytes
(0 = pas de support TRIM,
valeur non nulle = TRIM disponible)

Pour voir si fstrim s'exécute automatiquement :
systemctl status fstrim.timer

macOS : system_profiler SPSerialATADataType | grep -i 'TRIM Support'
```


PARTIE I — FONDATIONS PHYSIQUES

Chapitre 3

Systèmes de fichiers : la carte du trésor

3.1 Pourquoi le système de fichiers décide

Le système de fichiers (FS) est la couche logicielle qui transforme un bloc-périphérique brut (une succession de secteurs) en arborescence de fichiers et dossiers nommés. Il maintient pour cela des **structures internes** qui font le lien entre nom de fichier, métadonnées (taille, dates, permissions) et localisation physique des données sur le support.

Quand on supprime un fichier, le FS modifie typiquement deux ou trois de ces structures internes. Le contenu du fichier lui-même n'est pas touché. C'est cette dissymétrie qui rend possible la récupération logique : **les données brutes survivent à la suppression de leur entrée dans la « carte »**.

Mais chaque FS gère cette « carte » différemment. Certains conservent beaucoup de traces (NTFS, avec son journal $LogFile, est très bavard), d'autres peu (ext4 libère les inodes et extents assez agressivement). Cela se traduit en chances de récupération sensiblement différentes.

3.2 FAT32 et exFAT : la simplicité

Ce sont les FS les plus simples encore utilisés massivement, principalement sur les supports amovibles (clés USB, cartes SD, appareils photo, dashcams). FAT32 est limité à 4 Go par fichier ; exFAT (2006, Microsoft) lève cette limite et est devenu le standard inter-plateforme pour le stockage de masse.

Structure : un **boot sector** au début, une ou deux **tables FAT** qui décrivent la chaîne de clusters de chaque fichier, et le reste du volume en zone de données. Chaque fichier dans un répertoire est décrit par une entrée de 32 octets contenant nom court, attributs et premier cluster.

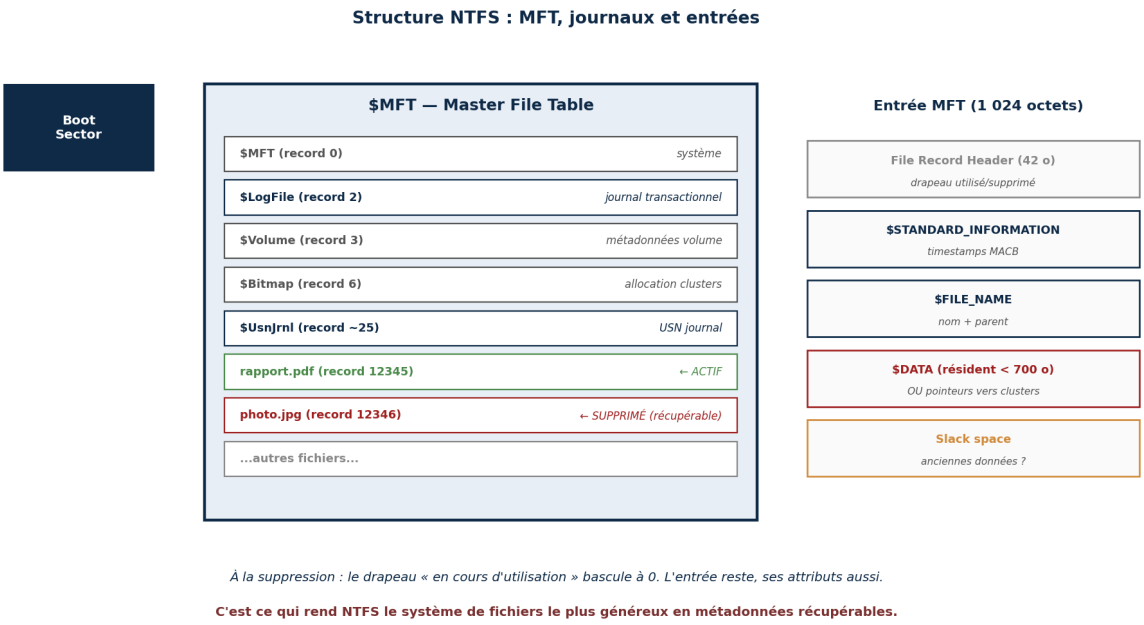
À la suppression :

- Le premier caractère de l'entrée de répertoire est remplacé par 0xE5, marquant l'entrée comme supprimée.
- Les clusters dans la table FAT sont marqués libres (remis à zéro).
- Le contenu des clusters lui-même reste intact jusqu'à réécriture.

La récupération est en général très efficace sur FAT/exFAT, surtout pour les fichiers contigus (peu de fragmentation, ce qui est fréquent sur des cartes SD utilisées en mode séquentiel). Limite principale : la première lettre du nom est perdue. Les outils mettent souvent un caractère générique (_) à la place.

3.3 NTFS : la richesse forensique

NTFS (*New Technology File System*, Microsoft, 1993) est le FS standard de Windows depuis Windows NT. C'est techniquement le FS le plus généreux en métadonnées résiduelles, ce qui en fait le plus récupérable d'un point de vue logique.



Structure NTFS : Boot Sector, $MFT et entrées de 1 024 octets contenant header + attributs.

Sa structure centrale est la **Master File Table** ($MFT) : un fichier spécial qui contient une entrée de 1 024 octets par fichier et par répertoire du volume. Cette entrée comprend :

- Un en-tête (42 premiers octets) avec un drapeau indiquant si l'entrée est utilisée ou supprimée.
- Un attribut $STANDARD_INFORMATION avec les quatre timestamps MACB (Modified, Accessed, Created, Birth/MFT change).
- Un attribut $FILE_NAME avec le nom et une référence au répertoire parent.
- Un attribut $DATA qui contient soit le contenu du fichier directement (s'il fait moins de ~700 octets, on parle d'attribut *résident*), soit une liste de *runs* pointant vers des clusters de données.

3.4 Corrélation temporelle multi-sources sur NTFS

La vraie puissance de NTFS en forensique se révèle quand on corrèle plusieurs sources de métadonnées :

- Les entrées **$MFT** et leurs deux jeux de timestamps (l'attribut $STANDARD_INFORMATION, modifiable par le système, et l'attribut $FILE_NAME, modifié uniquement à la création et au renommage). La divergence entre les deux est un marqueur classique de manipulation d'horodatage).
- Le journal transactionnel $LogFile qui conserve les dernières opérations sur le volume.
- Le journal d'USN $UsnJrnl:$J qui répertorie chaque création, modification, renommage et suppression avec horodatage et code de raison.
- Les **journaux d'événements Windows** (.evtx) qui tracent connexions, exécutions, accès — corrélables au niveau seconde.
- Le **registre** (UserAssist, ShellBags, MUICache) qui mémorise les exécutions et navigations dans l'Explorateur.

Workflow type : exporter le $MFT en CSV avec MFTECmd (Eric Zimmerman), le $LogFile avec LogFileParser, le $UsnJrnl avec UsnJrnl2Csv, fusionner ces flux dans un outil de timeline (Timeline Explorer, Timesketch, ou Plaso/log2timeline pour le côté open source) et reconstruire la séquence des événements. Cette approche multi-sources est indispensable dès qu'il y a enjeu judiciaire — un seul flux peut être manipulé, plusieurs flux concordants sont beaucoup plus difficiles à falsifier.

NTFS slack space — Pour la récupération de fichiers supprimés (sans enjeu judiciaire), NTFS reste le FS le plus permissif : l'entrée MFT reste après suppression, avec tous ses attributs et souvent ses pointeurs vers les clusters de données. Les outils comme MFTECmd savent en plus récupérer des fragments dans le **MFT slack space** — espace non utilisé à l'intérieur des entrées MFT, qui contient souvent des restes d'anciennes entrées (référence : Sygnia, *The Forensic Value of MFT Slack Space*, 2025).

3.5 ext4 : la spécificité Linux

ext4 (2008) est le FS par défaut de la plupart des distributions Linux. Trois éléments structurels clés :

- Le **superblock**, qui contient les paramètres globaux du FS (nombre total d'inodes, taille des blocs, etc.).
- La **table d'inodes**, qui contient une structure par fichier/dossier avec ses métadonnées.
- Les **extents** : ext4 ne décrit pas les blocs de données fichier par fichier (comme ext3 le faisait avec ses pointeurs indirects), mais par plages contigües (extents). Plus efficace pour les gros fichiers, mais plus destructeur à la suppression.

À la suppression d'un fichier sur ext4 :

1. L'inode est marqué libre dans le bitmap d'inodes.
2. Les extents sont libérés dans le bitmap de blocs.
3. Dans l'inode lui-même, ext4 efface partiellement les pointeurs vers les blocs (contrairement à ext3 qui les conservait). C'est ce qui rend la récupération plus difficile sur ext4 que sur ext3.

L'outil de référence est **extundelete** (open source), qui exploite le journal ext4 pour retrouver les anciennes versions des inodes supprimés avant que le journal lui-même ne les réécrive. Quand cela échoue, **debugfs** (inclus dans e2fsprogs) permet d'examiner manuellement la structure :

```
$ sudo debugfs /dev/sda1
debugfs: lsdel # liste les inodes récemment supprimés
debugfs: stat <12345> # détails de l'inode 12345
debugfs: dump <12345> /chemin/fichier.bin
```

Attention — Sur ext4, si vous venez de supprimer quelque chose d'important, remontez immédiatement la partition en lecture seule avant toute autre action : sudo mount -o remount,ro /dev/sdXY. Toute écriture, même un simple log système, peut réutiliser les inodes ou les blocs libérés.

3.6 APFS : copy-on-write et snapshots

APFS (*Apple File System*, 2017) a remplacé HFS+ sur macOS, iOS et iPadOS. C'est un FS moderne qui repose sur deux principes :

- **Copy-on-write.** Toute modification écrit ailleurs et met à jour les pointeurs ; les anciennes versions ne sont jamais directement écrasées. Cela garantit la cohérence en cas de coupure.
- **Snapshots.** APFS sait conserver des images instantanées d'état antérieur du volume, à coût marginal presque nul (puisque le copy-on-write conserve déjà les anciens blocs). Time Machine sur macOS s'appuie intensivement sur ce mécanisme.

Conséquence pour la récupération : sur un APFS non chiffré, des fichiers supprimés il y a des semaines peuvent être présents dans un snapshot local. Outils comme R-Studio, UFS Explorer et Disk Drill exploitent ces snapshots.

Le mur, c'est FileVault. Activé par défaut sur les Mac modernes avec puce Apple Silicon, FileVault chiffre tout le volume avec AES-256, et la clé est protégée par le mot de passe utilisateur et la *Secure Enclave*. Sans le mot de passe, la donnée physique sur le support n'est qu'un flux pseudo-aléatoire. Voir chapitre 13 pour les méthodes spécifiques aux Mac modernes.

3.7 Btrfs et ZFS : robustesse maximale

Btrfs (Oracle, intégré au noyau Linux depuis 2009) et ZFS (Sun Microsystems, 2006, désormais OpenZFS) sont deux FS de la famille « copy-on-write + checksums + snapshots », pensés pour la résilience à grande échelle. On les retrouve principalement sur les NAS (Synology, QNAP), les serveurs Linux et les appliances de stockage (TrueNAS).

- **Checksums.** Chaque bloc est protégé par une somme de contrôle. La détection silencieuse de corruption (*bit rot*) est intégrée.
- **Self-healing.** Sur un volume miroir ou RAID-Z, ZFS peut réécrire automatiquement un bloc corrompu à partir d'une copie saine.
- **Snapshots.** Comme APFS, à coût quasi nul, et exploités par les NAS modernes pour offrir aux utilisateurs des sauvegardes ponctuelles. Critique en post-ransomware : la plupart des ransomwares NAS chiffrent les fichiers visibles mais ne touchent pas aux snapshots Btrfs ou ZFS (voir chap. 12).

Pour la récupération : ces FS sont en pratique très peu vulnérables à la perte par corruption logique simple ; ils le sont par contre à la **fragmentation extrême** (le copy-on-write fragmente naturellement le contenu au fil des modifications) et à la complexité de leurs structures internes, ce qui rend le data carving classique très inefficace. L'approche la plus productive sur ces FS est presque toujours **via les snapshots**, pas via le carving.

3.8 Tableau de synthèse

FS	Plateformes	Comportement à la suppression	Qualité de récup. logique
FAT32	USB, SD, anciens systèmes	Entrée marquée 0xE5, FAT remise à zéro	Très bonne (perte 1re lettre)
exFAT	USB, SD haute capacité	Idem FAT32, capacité étendue	Très bonne
NTFS	Windows	MFT entry marquée supprimée, $LogFile et $UsnJrnl conservent des traces	Excellente — parfois lente
ext4	Linux	Inode libéré, extents effacés agressivement	Moyenne — extundelete dans fenêtre courte
APFS	macOS, iOS	Copy-on-write, snapshots conservés selon politique	Excellente via snapshots ; nulle si FileVault sans clé
Btrfs / ZFS	NAS, serveurs Linux	Copy-on-write, snapshots, checksums	Excellente via snapshots

Partie II

Diagnostic

Avant d'agir, comprendre. Deux chapitres : un panorama chiffré des causes de perte de données en 2025-2026, et une méthode de triage pour décider si vous êtes face à un cas logique ou physique, et si vous pouvez intervenir vous-même ou si l'envoi en laboratoire s'impose.

PARTIE II — DIAGNOSTIC

Chapitre 4

Causes de perte : les chiffres 2025-2026

4.1 Quatre familles de causes

On classe les pertes en quatre catégories qui appellent des réponses très différentes :

- **Humaines et logiques** : suppression accidentelle, formatage, mauvaise manipulation, erreur de configuration. Le support est sain ; les données sont logiquement inaccessibles mais physiquement présentes.
- **Cyber** : ransomware, malware destructeur, wiper, suppression malveillante. Le ransomware ajoute une couche de chiffrement ; les wipers (NotPetya par exemple) détruisent réellement.
- **Matérielles** : panne mécanique (HDD), défaillance électronique (PCB grillé), usure NAND (SSD).
- **Environnementales** : incendie, inondation, surtension, vol, destruction physique.

4.2 Le ransomware, la nouvelle norme

Le rapport Verizon DBIR 2025 est la référence statistique sur les compromissions de données. Sur la période couverte (novembre 2023 à octobre 2024), Verizon a analysé plus de 22 000 incidents et 12 195 compromissions confirmées.

Indicateur	Valeur 2024 (DBIR 2025)	Tendance
Ransomware dans les breaches	44 %	+37 % vs DBIR 2024
Ransomware dans breaches PME	88 %	Aggravation
Ransomware dans grandes entreprises	39 %	Stable
Identifiants volés (vecteur initial)	22 %	Toujours n° 1
Vulnérabilités exploitées	20 %	+34 %
Implication d'un tiers (supply chain)	30 %	Doublé
Médiane des rançons payées	115 000 $	En baisse
Refus de payer la rançon	64 % des victimes	+14 pts en 2 ans

Source : Verizon Business, 2025 Data Breach Investigations Report, publié le 23 avril 2025.

Deux lectures opposées du même rapport. La pessimiste : le ransomware est devenu un mode opératoire dominant, particulièrement dévastateur pour les PME qui en sont victimes dans neuf cas sur dix. L'optimiste : la médiane des rançons baisse, deux victimes sur trois refusent désormais de payer.

4.3 L'erreur humaine, toujours majoritaire

L'élément humain (au sens large : erreur, abus de privilège, ingénierie sociale) reste impliqué dans une part dominante des compromissions. Le DBIR 2025 chiffre cela à 60 % sur l'ensemble des breaches étudiés. Les définitions varient d'un rapport à l'autre — certains atteignent 95 % en incluant toute action humaine en amont de l'incident — mais l'ordre de grandeur est constant.

Pour la récupération de données spécifiquement, les causes humaines les plus fréquemment rencontrées par les laboratoires sont la suppression accidentelle de fichiers ou de répertoires, le formatage par erreur (souvent au moment de l'installation d'un OS), l'écrasement de fichiers par mauvaise manipulation, la suppression massive par script ou commande, et la perte de mot de passe ou de clé de chiffrement.

4.4 La fiabilité matérielle moyenne

Pour les pannes matérielles sur HDD, Backblaze reste la référence publique avec son rapport *Drive Stats 2025*. Sur 337 192 disques de production fin 2025, AFR annuel global de 1,36 %. AFR cumulé sur la vie des disques (lifetime) : 1,30 %. Pour les SSD, aucun rapport public comparable n'existe à grande échelle ; l'endurance théorique des SSD modernes (TBW garanti par les constructeurs) couvre normalement 5 à 10 ans d'usage consumer ; la panne effective est souvent due à un contrôleur défaillant ou un firmware corrompu, pas à l'usure des cellules.

4.5 Synthèse

1. L'**erreur humaine** reste la cause numéro un en volume, particulièrement chez les particuliers et les PME.
2. Le **ransomware** a explosé pour devenir la première cause en termes d'impact financier — il est désormais présent dans près d'une compromission sur deux en entreprise.
3. Les **pannes matérielles** sont en lente diminution sur HDD (meilleure qualité, AFR sous les 1,5 %) ; sur SSD, elles sont moins fréquentes mais souvent plus catastrophiques.
4. Les **incidents environnementaux** représentent quelques pourcents des cas, mais leur coût peut être colossal.

PARTIE II — DIAGNOSTIC

Chapitre 5

Diagnostic et triage

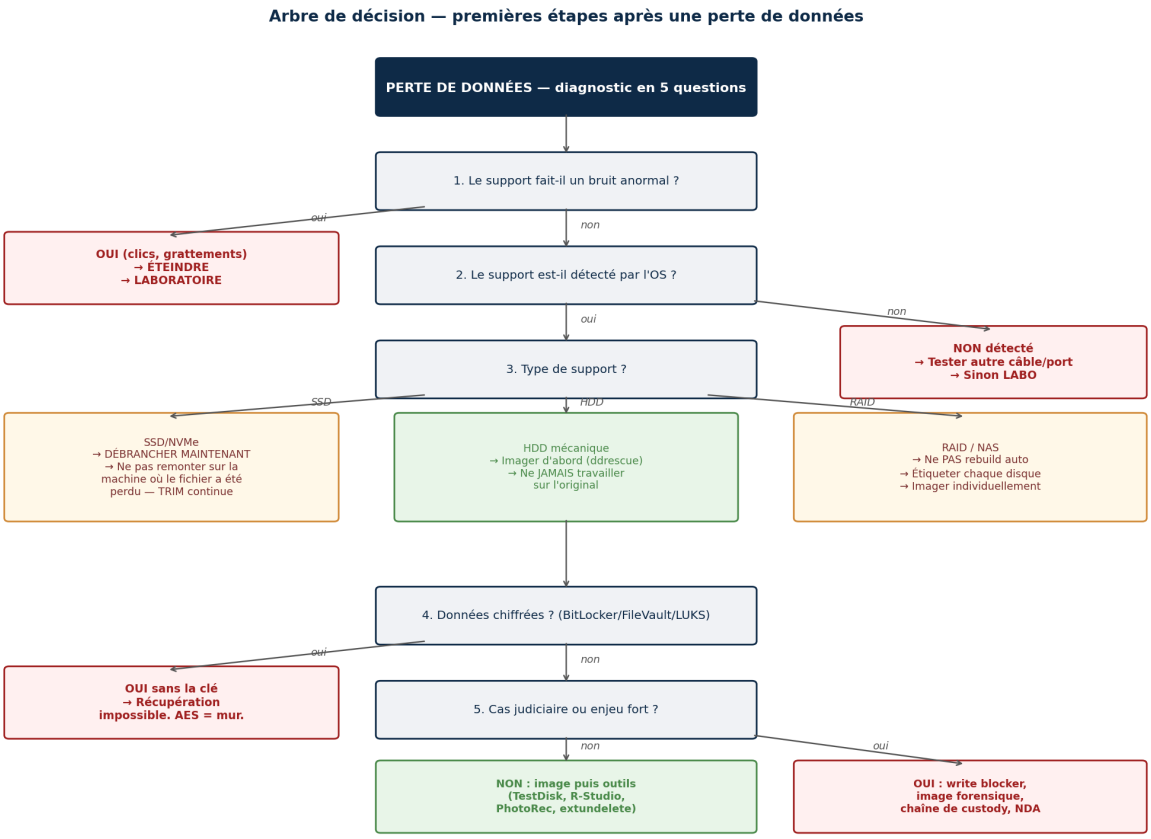
5.1 Pourquoi le diagnostic est l'étape critique

Le diagnostic décide de tout : du choix entre intervention logicielle ou physique, du choix entre tentative personnelle ou envoi en laboratoire, du coût et du délai prévisibles, et souvent du résultat lui-même. Un mauvais diagnostic conduit à des actions inadaptées qui aggravent la situation.

> **Attention —** Tant que le diagnostic n'est pas posé, ne touchez à rien. Surtout, ne lancez aucun outil de récupération « pour voir » : beaucoup d'entre eux écrivent sur le support source dès qu'on les installe ou dès le premier scan.

5.2 Procédure de triage en cinq étapes

1. **Observer.** Le support est-il alimenté ? Émet-il du bruit ? Lequel ? Est-il chaud ? Le BIOS/UEFI le détecte-t-il ? L'OS l'affiche-t-il dans les outils standards (Gestionnaire de disques Windows, Utilitaire de disque macOS, lsblk Linux) ? Notez tout sans rien modifier.
2. **Classer.** À partir des observations, classer en : *physique* (non détecté, bruits anormaux, surchauffe), *logique* (détecté mais inaccessible, fichiers manquants, FS corrompu), ou *hybride* (détection intermittente, lecture partielle).
3. **Évaluer l'enjeu.** Les données sont-elles irremplaçables ? Ont-elles une valeur judiciaire, médicale, professionnelle ? Existent-elles ailleurs (sauvegarde, cloud) ? L'urgence est-elle réelle ?
4. **Décider du chemin.** Selon la combinaison (type / enjeu / compétences disponibles), choisir : intervention personnelle, intervention par un technicien IT généraliste, ou envoi en laboratoire spécialisé.
5. **Documenter.** Si l'enjeu peut devenir judiciaire, photographier l'état du support, noter les numéros de série, tracer chaque manipulation. C'est la chaîne de custody (voir chapitre 14).



Arbre de décision rapide après une perte de données : les cinq premières questions qui orientent la suite.

5.3 Symptômes typiques et leur signification

Symptôme observé	Diagnostic probable	Action immédiate
Clics répétés sur HDD	Têtes HS — physique	Éteindre immédiatement, ne pas rebrancher
HDD silencieux, non détecté	PCB ou moteur HS — physique	Éteindre, envoi labo
HDD détecté avec capacité absurde (0, 8 Mo)	Service Area corrompue	Envoi labo (PC-3000)
HDD détecté, grandes lenteurs	Secteurs défectueux — physique évolutif	Imagerie d'urgence avec ddrescue
SSD non détecté du tout	Contrôleur HS — physique	Éteindre, envoi labo (JTAG/chip-off)
SSD détecté, capacité bizarre (8 Mo, 0 Mo)	Firmware corrompu — physique	Envoi labo
Partition manquante, table corrompue	Logique	Image ddrescue puis TestDisk
Fichiers supprimés par erreur sur HDD	Logique — fenêtre large	Débrancher, image, R-Studio
Fichiers supprimés sur SSD	Logique — fenêtre courte (TRIM)	DÉBRANCHER IMMÉDIATEMENT
Volume RAW (NTFS/exFAT corrompu)	Logique	Image puis R-Studio/UFS Explorer
Fichiers chiffrés extensions inconnues	Ransomware	Voir chapitre 12
Demande de mot de passe sur tout le disque	BitLocker/FileVault/LUKS	Trouver la clé de récupération

5.4 Quand passer en laboratoire

Trois critères, dont au moins un suffit :

- Le support n'est pas détecté, ou émet des bruits anormaux → physique → labo.
- Les données sont irremplaçables et critiques (médical, judiciaire, professionnel à fort enjeu) → labo, même si le cas semble simple.
- Vous avez déjà tenté quelque chose qui a aggravé la situation → arrêtez, et laissez un pro évaluer ce qui reste récupérable.

5.5 Choisir un laboratoire

Critères de sérieux à vérifier auprès d'un laboratoire :

- Salle blanche ISO 5 certifiée (demander le certificat ISO 14644-1).
- Diagnostic gratuit et paiement au résultat — standard de marché en 2026.
- Liste des fichiers récupérables communiquée avant paiement (DAFOTEC parle de service « VeriFiles » : le client valide explicitement la liste des fichiers issue du diagnostic avant que le forfait ne soit facturé).
- Confidentialité écrite (NDA), surtout pour les cas professionnels.
- Réputation vérifiable (avis indépendants type Ekomi/Trustpilot, publications techniques, mentions dans la presse spécialisée). Pour les références internationales : Ontrack, Kroll, DriveSavers, SalvageData, Gillware, Secure Data Recovery. Pour la France : DAFOTEC à Roubaix (laboratoire ISO 5 depuis 2004, clients institutionnels publics : Gendarmerie Nationale, CHU Tourcoing, CNRS, INSERM, universités françaises).

Signes de laboratoire douteux — Si on vous demande un règlement intégral avant diagnostic, ou qu'on vous promet un taux de succès garanti, partez. Aucun laboratoire sérieux ne promet une récupération avant d'avoir ouvert le support.

Partie III

Méthodes

Six chapitres qui constituent le cœur opérationnel du livre : comment imager un support (la fondation de toute autre opération), comment analyser la couche logique, comment sculpter des fichiers à partir de données brutes (carving), comment intervenir physiquement sur un disque dur et sur un SSD, et comment gérer les configurations RAID.

Trois règles d'or — Trois règles transversales valent pour tous ces chapitres et ne seront pas répétées à chaque page : (1) **imager d'abord**, travailler ensuite sur l'image ; (2) **ne jamais écrire sur le support source**, ni installer un logiciel dessus, ni récupérer des fichiers dessus ; (3) sur SSD avec TRIM, **chaque seconde sous tension réduit la fenêtre** — débrancher tôt vaut mieux que diagnostiquer tard.

PARTIE III — MÉTHODES

Chapitre 6

Imagerie sécurisée

6.1 Le principe

L'imagerie consiste à créer une copie bit à bit du support source vers un fichier image, puis à travailler exclusivement sur cette image. L'original est mis de côté, à l'abri.

Trois raisons :

1. **Sauvegarder ce qui peut l'être.** Un support qui tombe en panne en fait souvent plus pendant les heures suivantes. La première lecture peut être la dernière qui réussit.
2. **Travailler sereinement.** Sur l'image, on peut faire autant d'essais qu'on veut. Si un outil corrompt quelque chose, on en crée une autre copie.
3. **Préserver la preuve.** En forensique, l'original est scellé avec son hash de référence ; tout travail se fait sur une copie hashée elle aussi. C'est ce qui rend la procédure recevable en justice (norme ISO 27037).

6.2 ddrescue : l'outil de référence

GNU ddrescue (paquet gddrescue sous Debian, Ubuntu, et la plupart des distributions Linux) est l'outil open source de référence. Sa supériorité sur dd classique tient à trois éléments :

- Un fichier de carte (*mapfile*) qui enregistre précisément les zones déjà copiées, à recopier, lentes ou échouées. Il permet de reprendre exactement où on s'était arrêté, et de programmer des passes ciblées.
- Une stratégie de lecture en plusieurs passes : rapide d'abord (on saute les zones lentes), agressive ensuite (on revient sur les zones difficiles).
- Une gestion fine des secteurs en erreur, avec nombre maximal de tentatives configurable.

Workflow type

Identifier le périphérique avec précision avant tout autre chose. Une erreur de lettre, et c'est un disque sain qui est écrasé.

```
$ lsblk -o NAME,SIZE,MODEL,SERIAL,TRAN
NAME SIZE MODEL SERIAL TRAN
sda 500G ST500LM030-2E717D WCC6Y0L1234 sata
sdb 2T WDC_WD20EZRZ WD-WCC4M1234 usb
...

# Le serial number permet de confirmer qu'on vise le bon disque.
```

Première passe, rapide : on copie ce qui se lit facilement, on saute le reste.

```
$ sudo ddrescue -f -n -d /dev/sdX /chemin/image.img /chemin/image.map

-f : autorise la sortie vers un device
-n : 'no-scrape' : ne s'attarde pas sur les zones difficiles
-d : accès direct au device (bypass cache OS)
```

Deuxième passe, ciblée sur les zones difficiles avec quelques tentatives :


```
$ sudo ddrescue -f -d -r3 /dev/sdX /chemin/image.img /chemin/image.map

-r3 : jusqu'à 3 retries par secteur en erreur
```

Sur un disque qui claque (têtes HS), on évite d'aller plus haut que -r3 : chaque tentative supplémentaire est une occasion de plus d'endommager la surface. Sur un disque dont le problème est juste électronique, on peut aller jusqu'à -r10 sans risque physique.

Option utile sur les cas particulièrement abîmés : passe en lecture inverse, qui aide quand l'ordre de présentation des secteurs joue (positionnement difficile sur certains cylindres) :

```
$ sudo ddrescue -f -d -R -r3 /dev/sdX /chemin/image.img /chemin/image.map

-R : 'reverse' : lit de la fin vers le début
```

Une fois l'image obtenue

```
$ sha256sum /chemin/image.img > /chemin/image.img.sha256

# Pour explorer l'image en lecture seule :
$ sudo losetup --read-only --find --show /chemin/image.img
/dev/loop0

# Sur ext4 : noload empêche le rejeu de journal (qui écrirait)
$ sudo mount -o ro,noload /dev/loop0 /mnt/recup

# Sur NTFS via ntfs-3g :
$ sudo mount -t ntfs-3g -o ro,norecover /dev/loop0 /mnt/recup

# Démonter et libérer le loop quand on a fini :
$ sudo umount /mnt/recup
$ sudo losetup -d /dev/loop0
```

Attention — Stockez le mapfile et l'image sur un support distinct du source. Si l'image est sur la même clé USB que le support en panne, et que cette clé tombe, on a tout perdu. Toujours sur un disque sain, rapide et avec assez de place.

6.3 Alternatives à ddrescue

FTK Imager (AccessData/Exterro, gratuit). Outil Windows très populaire en forensique. Crée des images au format E01 (EnCase) ou DD brut, calcule MD5/SHA1/SHA256 automatiquement, supporte les write blockers hardware.

Guymager (Linux, GUI). Interface graphique pour la création d'images forensiques. Plus pratique que ddrescue pour les utilisateurs occasionnels mais moins flexible sur les cas difficiles.

dc3dd (DoD Cyber Crime Center). Variante de dd améliorée pour la forensique : hash à la volée, journalisation, validation.

Outils hardware : PC-3000 Disk Imager (ACE Lab), DeepSpar Disk Imager, Atola Insight Forensic. Ces solutions hardware gèrent les supports gravement endommagés mieux que les outils purement logiciels (contrôle direct du contrôleur, gestion fine des resets, masquage des têtes HS sur HDD). Réservés aux laboratoires en raison du coût.

6.4 Write blockers

Pour les cas forensiques, on intercale entre le support source et la machine d'analyse un **write blocker** matériel : un dispositif qui laisse passer les lectures mais bloque physiquement toute écriture. Marques de référence : Tableau (OpenText), WiebeTech (CRU).

Pour un usage non forensique mais prudent, le write blocker logiciel via blockdev --setro sous Linux suffit en pratique.

PARTIE III — MÉTHODES

Chapitre 7

Analyse logique et réparation FS

7.1 Le principe

Une fois l'image obtenue, l'analyse logique cherche à **réparer ou interpréter les structures du système de fichiers** présentes sur l'image, plutôt que de chercher directement des fichiers dans les données brutes. C'est presque toujours plus efficace que le carving : on récupère non seulement le contenu, mais aussi les noms, les dates, l'arborescence.

7.2 TestDisk : la table de partition

TestDisk (Christophe Grenier, CGSecurity) est l'outil de référence pour la réparation de tables de partition MBR et GPT, et pour la récupération de partitions effacées. Multiplate-forme.

Workflow sur une image qui a perdu sa table :

1. Lancer testdisk /chemin/image.img.
2. Choisir « None » pour la création de log.
3. Sélectionner le disque/image, puis le type de table.
4. Lancer « Analyse » puis « Quick Search ».
5. Si Quick Search ne suffit pas, lancer « Deeper Search ».
6. Vérifier les partitions trouvées, puis écrire la table (« Write »).

7.3 NTFS : MFT, $LogFile, $UsnJrnl

- **R-Studio** et **UFS Explorer** (commerciaux) sont les références pour la reconstruction NTFS.
- **MFTECmd** (Eric Zimmerman, gratuit) parse le fichier $MFT en CSV exploitable.
- **LogFileParser** et **UsnJrnl2Csv** (Eric Zimmerman) exploitent les journaux.
- **The Sleuth Kit** (TSK) et son interface **Autopsy** offrent un cadre complet, open source.

```
# Avec The Sleuth Kit : lister tous les fichiers, y compris supprimés
$ fls -r -p /chemin/image.img > fichiers.txt
# Les fichiers supprimés sont marqués '*' au début de la ligne

# Récupérer un fichier supprimé par son inode
$ icat /chemin/image.img 12345 > fichier_recup.bin
```


7.4 ext4 : extundelete, debugfs, ext4magic

```
# Restaurer un fichier précis dont on connaît le nom
$ sudo extundelete --restore-file 'home/user/important.pdf' /dev/sdb1

# Restaurer tout ce qui est récupérable
$ sudo extundelete --restore-all /dev/sdb1

# Avec debugfs, lister les inodes supprimés
$ sudo debugfs /dev/sdb1
debugfs: lsdel
Inode Owner Mode Size Blocks Time deleted
1234 1000 100644 524288 128 Sun May 4 14:32:11 2026
debugfs: dump <1234> /tmp/recovered
debugfs: quit
```

7.5 APFS : exploiter les snapshots

```
# Lister les snapshots APFS sur un Mac vivant
$ tmutil listlocalsnapshots /

# Lister les snapshots sur un volume monté en lecture seule
$ diskutil apfs listSnapshots /Volumes/data
```

R-Studio et UFS Explorer Professional savent exploiter les snapshots APFS — y compris à partir d'une image brute.

7.6 Btrfs et ZFS : snapshots et récupération

```
# Lister les snapshots Btrfs
$ sudo btrfs subvolume list /volume1

# Restaurer un fichier depuis un snapshot
$ cp /volume1/.snapshots/123/fichier.pdf /volume1/fichier.pdf

# Sur ZFS, c'est encore plus direct :
$ sudo zfs list -t snapshot
$ ls /pool/dataset/.zfs/snapshot/snapshot_name/
```

Sur les NAS Synology DSM 7 / QNAP QTS 5 modernes, les snapshots Btrfs sont activés par défaut. C'est la raison pour laquelle les attaques ransomware de type eCh0raix, QlockerBunny ou DeadBolt peuvent souvent être contournées sans payer : le ransomware chiffre les fichiers visibles mais ne touche pas aux snapshots en lecture seule (chapitre 12).

PARTIE III — MÉTHODES

Chapitre 8

Data carving en profondeur

8.1 Quand carver

Le data carving reconstitue des fichiers en cherchant leurs signatures binaires dans les données brutes, **sans utiliser les structures du système de fichiers**. Opération de dernier recours quand la couche logique est trop endommagée.

Cas typiques : formatage complet (structure FS réécrite), image brute issue d'un chip-off, réinstallation d'OS qui a écrit son nouveau système sur l'ancien, support tellement corrompu que les outils logiques ne trouvent rien.

8.2 Quatre niveaux de sophistication

Niveau 1 — Signature simple (header / footer)

L'approche historique. On scanne le support à la recherche d'un *magic number* caractéristique du début du format, puis on lit jusqu'au magic de fin ou jusqu'à une taille maximale fixée.

Format	Header (hex)	Footer / fin
JPEG (JFIF)	FF D8 FF E0	FF D9
JPEG (Exif)	FF D8 FF E1	FF D9
PNG	89 50 4E 47 0D 0A 1A 0A	49 45 4E 44 AE 42 60 82
PDF	25 50 44 46 ("%PDF")	25 25 45 4F 46 ("%%EOF")
ZIP / DOCX / XLSX	50 4B 03 04	Variable
MP4 / MOV	(offset 4) 66 74 79 70	Pas de footer fixe
RAR (v5+)	52 61 72 21 1A 07 01 00	Variable
SQLite	53 51 4C 69 74 65 20 66 6F 72 6D 61 74 20 33 00	

Très efficace sur des fichiers **non fragmentés**. Échoue dès qu'un fichier est fragmenté. Outils : **PhotoRec**, **Foremost**, **Scalpel**.

Niveau 2 — Carving sémantique (structure-aware)

On exploite la structure interne du format. Pour un PDF, la table xref. Pour un ZIP, le central directory. Cela permet de reconstituer des fichiers fragmentés.

Niveau 3 — Analyse d'entropie

Calculer l'entropie de Shannon par bloc pour distinguer texte / données compressées / données chiffrées et cibler le carving.

Niveau 4 — Apprentissage automatique

Les approches récentes (2023-2026) utilisent des réseaux de neurones pour classifier et réassembler. Belkasoft X et Magnet AXIOM annoncent des modules ML depuis 2024-2025. Résultats prometteurs sur certains formats, en pratique limités.

8.3 PhotoRec : le standard open source

```
# Lancer PhotoRec sur une image
$ sudo photorec /chemin/image.img
```

Étapes : choisir le support, type de table, partition, FS d'origine, **File Opt** pour ne sélectionner que les types voulus, répertoire de sortie. PhotoRec est lent : compter plusieurs heures pour 1 To.

Attention — PhotoRec ne récupère **jamais** les noms d'origine — il les renomme en f0000001.jpg, etc. Pour un usage forensique sérieux, préférer une approche FS-aware (ch. 7) quand c'est possible.

8.4 Limites dures du carving

- **Fragmentation.** Sur des FS très fragmentés (ext4 ancien, ZFS/Btrfs copy-on-write), les fichiers sont éclatés. Le carving signature simple récupère le premier fragment puis du bruit.
- **Chiffrement.** Du contenu chiffré a une entropie maximale et ne ressemble à aucun format connu.
- **Compression.** Un fichier ZIP, MP3 ou JPEG qui a perdu ses premiers blocs est irrécupérable même si le reste est intact.
- **Faux positifs.** Sur 1 To de NAND brute issue de chip-off, le carving peut produire des millions de fichiers, dont 99 % sont du bruit.

PARTIE III — MÉTHODES

Chapitre 9

Intervention physique sur HDD

9.1 La salle blanche : pourquoi c'est non-négociable

Les têtes d'un HDD volent à quelques nanomètres au-dessus de la couche magnétique. Une poussière atmosphérique ambiante (5 à 50 microns typiquement) coincée sous une tête en mouvement, c'est l'équivalent à l'échelle d'une voiture roulant à 200 km/h et heurtant un mur de béton. La couche magnétique est rayée, souvent de façon irrécupérable.

Pour ouvrir un disque dur sans détruire les plateaux, il faut un environnement où la concentration en particules est drastiquement réduite. La norme ISO 14644-1 classe les salles blanches par concentration maximale de particules :

Classe ISO	Particules >=0,5 micron / m<super>3</super>	Usage typique
ISO 1	10	Fabrication semiconducteurs ultra-précise
ISO 2	100	Recherche pointe
ISO 3	1 000	Salle blanche avancée
ISO 4	10 000	Fabrication semiconducteurs standard
ISO 5	100 000	Récupération HDD professionnelle
ISO 6	1 000 000	Insuffisant pour HDD
Air ambiant	~35 000 000 (poussiéreux à propre)	Hors-sujet

La norme pour la récupération HDD est ISO 5. C'est ce qu'on trouve chez les laboratoires sérieux internationaux (DriveSavers, SalvageData, Gillware, Secure Data Recovery, Ontrack) et en France chez DAFOTEC à Roubaix.

Attention — L'ouverture d'un HDD dans une pièce ordinaire, même propre, est une garantie quasi-certaine de destruction supplémentaire. Les vidéos YouTube montrant des amateurs faisant un head swap dans leur garage sont irresponsables : elles ignorent l'environnement à 35 millions de particules par m^3 et survalorisent les rares cas où ça marche malgré tout.

9.2 Head swap (greffe de têtes)

Quand les têtes sont HS (par usure ou choc), on les remplace par celles d'un disque **donneur** physiquement identique. Procédure :

1. Diagnostic confirmant que la mécanique des plateaux est intacte et qu'on est bien face à un problème de têtes (clics typiques, amplitude de signal lecture anormale au démarrage).
2. Sourcing d'un disque donneur strictement identique. Les laboratoires gardent un stock de centaines de modèles, ou les achètent à des grossistes spécialisés.
3. Ouverture des deux disques sous flux laminaire, démontage des ensembles têtes/bras à l'aide d'outils dédiés (clés spécifiques, séparateurs de têtes pour éviter qu'elles se touchent quand elles

sont hors du disque).

4. Transfert de l'ensemble têtes/bras du donneur vers le patient.
5. Refermeture du patient, remise sous tension.
6. Imagerie immédiate avec un imager hardware (PC-3000, DeepSpar), avant que la nouvelle combinaison ne s'use à son tour.

Le donneur doit être identique jusqu'à la révision firmware. Un donneur de modèle apparemment identique mais d'une autre révision de firmware peut donner un disque qui tourne mais ne lit rien : la calibration têtes/firmware est figée au fabricant.

9.3 PCB swap et reprogrammation ROM

Si la panne est sur le circuit imprimé extérieur (surtension, TVS grillé), on peut remplacer le PCB par celui d'un donneur. Mais attention : sur la plupart des disques modernes, des paramètres de calibration spécifiques au support physique (carte des secteurs défectueux, paramètres têtes, etc.) sont stockés dans une ROM sur le PCB. Sans transfert de cette ROM (par dessoudage et resoudage, ou via PC-3000), le disque patient avec un PCB de donneur produira au mieux des données illisibles.

PC-3000 permet aussi de reprogrammer directement la ROM via une connexion COM/UART aux points de test du PCB. C'est rapide et non destructif.

9.4 Cas particuliers

9.4.1 Disques SMR

Les disques en SMR (voir 1.3) posent des défis spécifiques. Quand le firmware ou la zone de translation est corrompu, on ne peut pas simplement lire les plateaux : il faut reconstruire le mapping LBA → emplacement physique en tenant compte du cache et des bandes. PC-3000 a publié des modules SMR dédiés à partir de 2020. Le taux de succès reste inférieur à celui des CMR équivalents.

9.4.2 Stiction

Quand les têtes restent collées au plateau au démarrage, on peut tenter de « décoller » manuellement dans la salle blanche en faisant tourner les plateaux à la main pendant qu'on applique brièvement l'alimentation. Très délicat — on risque d'arracher la couche magnétique sous les têtes.

9.4.3 Plateaux rayés

Si la rayure est superficielle et localisée, on peut souvent récupérer ce qui est en dehors de la zone rayée (avec des secteurs perdus). Si la rayure est profonde ou étendue, c'est terminal — la couche magnétique a été arrachée, les données n'y sont plus.

Certains laboratoires extrêmement spécialisés pratiquent le **platter swap** : transfert des plateaux d'un disque patient vers un boîtier mécanique de donneur. C'est techniquement le plus délicat (déplacer un plateau sans désynchroniser sa position relative aux têtes est presque impossible) et le taux de succès est faible. À réserver aux cas extrêmes avec enjeu très fort.

9.5 Plateformes hardware professionnelles

Trois plateformes dominent :

- **PC-3000** (ACE Lab, Russie) : standard mondial de facto. Modules pour HDD, SSD, Flash, RAID, mobile. Base de connaissances par contrôleur et firmware tenue à jour.
- **DeepSpar Disk Imager** (Canada) : alternative très efficace pour l'imagerie HDD avec contrôle bas-niveau (head bypass, configuration de timeouts précis).
- **Atola Insight Forensic** : forensique avancée avec imagerie multi-passes et détection automatique des têtes défaillantes.

L'équipement complet d'un laboratoire (PC-3000 HDD + Flash + Express + adaptateurs + outils micro-soudure + salle blanche ISO 5) représente un investissement de plusieurs dizaines de milliers d'euros. C'est la raison principale pour laquelle la récupération physique est facturée à plusieurs centaines d'euros minimum dans tout laboratoire sérieux.

PARTIE III — MÉTHODES

Chapitre 10

Intervention physique sur SSD

10.1 Pourquoi c'est plus difficile qu'un HDD

Sur un HDD, la donnée est magnétique et persistante. Si on arrive à faire tourner les plateaux et à les lire (par head swap, PCB swap, etc.), on accède aux bits tels qu'ils ont été écrits.

Sur un SSD, la donnée est :

- Électrique (charge piégée dans des cellules), donc potentiellement volatile dans le temps si elle n'est pas rafraîchie.
- Embrouillée (*scrambled*) par le contrôleur pour équilibrer les charges électriques — il faut savoir désembrouiller.
- Codée par un ECC propre au contrôleur — il faut savoir décoder.
- Mappée logiquement par une **Flash Translation Layer** (FTL) que seul le contrôleur d'origine connaît parfaitement.
- Souvent chiffrée matériellement (SED, TCG Opal) par une clé que seul le contrôleur d'origine peut déverrouiller.

Trois techniques d'intervention, par ordre de préférence (la moins destructive d'abord) :

10.2 JTAG / ISP : non destructif

Les contrôleurs SSD modernes exposent souvent des points de test correspondant à un protocole de débogage interne : **JTAG** (Joint Test Action Group) ou **ISP** (In-System Programming). En soudant temporairement des fils fins sur ces points, et en connectant à un programmeur dédié, on peut :

- Lire le firmware du contrôleur.
- Injecter un *loader* de récupération qui court-circuite le firmware mort et accède directement à la NAND via les capacités du contrôleur.
- Sur certaines configurations, faire parler le contrôleur comme s'il fonctionnait normalement, et imager via SATA ou NVMe.

Avantages : la NAND est lue par son contrôleur d'origine, donc désembrouillage et ECC sont gérés automatiquement, et le chiffrement matériel reste déchiffré si la clé est présente. Le support physique n'est pas détruit.

Inconvénients : nécessite des outils spécialisés (PC-3000 Flash avec adaptateurs JTAG, ou solutions tierces comme RTPro, Medusa Pro), de bonnes compétences en micro-soudure de précision, et la connaissance des points de test pour chaque famille de contrôleurs. PC-3000 maintient une base de schémas par contrôleur, accessible aux labos sous contrat.

10.3 Chip-off : la technique de dernier recours

Si JTAG échoue ou n'est pas applicable (contrôleur mort, points de test absents), on désoude physiquement les puces NAND pour les lire indépendamment du contrôleur.

10.3.1 La dépose physique

Les puces NAND modernes sont en boîtier BGA (Ball Grid Array) avec des dizaines à plusieurs centaines de billes de soudure sous le composant. Le désouder requiert :

- Une station de rework à air chaud calibré avec profil thermique précis (rampe de chauffe contrôlée pour ne pas fissurer la puce ni détruire le PCB).
- Une protection thermique du reste du PCB (kapton, écrans thermiques).
- Un microscope binoculaire pour repositionner les puces sur des sockets de lecture.

10.3.2 La lecture

Une fois la puce désoudée et nettoyée (billes refaites au besoin), elle est lue sur un programmeur NAND universel : PC-3000 Flash, Soft-Center Flash, FlashExtractor. Ces programmeurs lisent les pages brutes telles qu'elles sont physiquement stockées.

10.3.3 La reconstruction logique (le vrai défi)

À ce stade, on a un dump brut de chaque puce NAND. Pour en extraire des données utilisables, il faut :

1. **Désembrouiller** (descrambler) les pages. Le contrôleur d'origine appliquait un XOR avec une séquence pseudo-aléatoire dépendant de l'adresse pour équilibrer les charges. Sans connaître le polynôme du LFSR (Linear Feedback Shift Register) utilisé, impossible d'inverser.
2. **Décoder l'ECC**. Les contrôleurs modernes utilisent du LDPC à plusieurs centaines de bits de parité par page. Sans reproduire ce pipeline, on ne corrige pas les erreurs de lecture et on perd beaucoup de données.
3. **Réassembler les pages**. Sur les SSD multi-puces, les pages logiques sont distribuées entre les puces selon un schéma d'entrelacement propre au contrôleur. Il faut reconstruire cet ordre.
4. **Reconstruire la FTL**. À partir des métadonnées intégrées à chaque page (spare area), reconstituer la table de mapping LBA → emplacement physique. C'est le travail le plus complexe.
5. **Si le SSD était chiffré matériellement**, et qu'on n'a pas pu récupérer la clé du contrôleur — c'est fini. Le contenu lisible est du chiffré.

Cette reconstruction est ce qui fait qu'un chip-off complet sur un SSD moderne peut prendre des semaines en laboratoire, et que le coût est élevé (les laboratoires comme DAFOTEC affichent des forfaits jusqu'à 950 € HT pour les pannes complexes).

10.4 Cas Apple Silicon : la difficulté maximale

Les Mac avec puce T2 (2018+) ou Apple Silicon M1/M2/M3/M4 intègrent le contrôleur SSD dans la puce CPU/SoC elle-même. Concrètement :

- La NAND est soudée directement sur la carte mère (pas de SSD amovible).
- Le contrôleur SSD est dans le SoC.
- Le chiffrement matériel est lié à un identifiant unique de la **Secure Enclave** du SoC.
- FileVault est activé par défaut sur Apple Silicon.

Pour une récupération sans le mot de passe utilisateur, c'est impossible : la clé est protégée par la Secure Enclave. Si le mot de passe est connu mais que la carte mère est défaillante, les laboratoires spécialisés peuvent en dernier recours transplanter les composants critiques (CPU/SoC contenant la

Secure Enclave) sur une carte mère donneuse vierge pour préserver la cohérence cryptographique, puis lire les NAND. DAFOTEC documente publiquement cette intervention sous le nom « CPU Swap mobile » pour smartphones, et applique des techniques comparables sur Mac à SSD soudé.

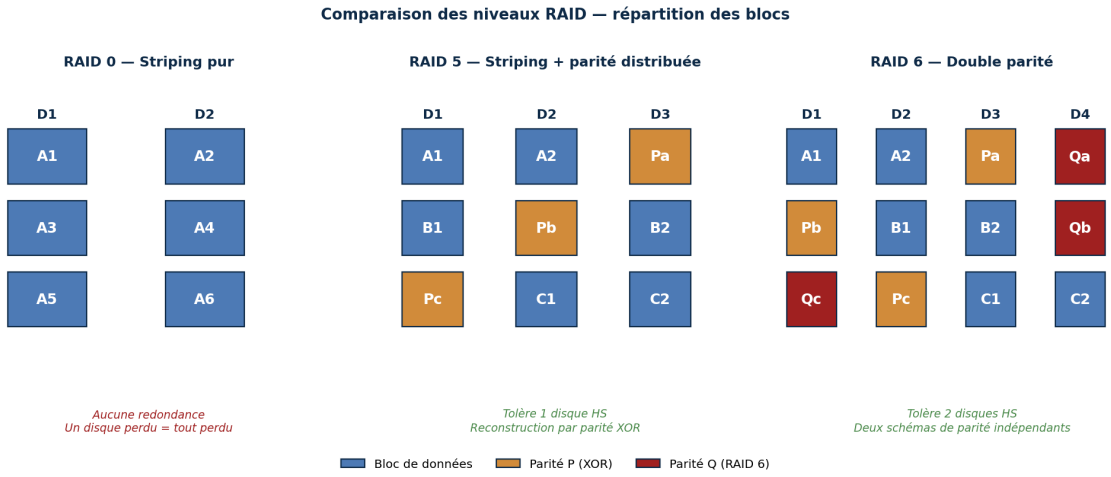
PARTIE III — MÉTHODES

Chapitre 11

RAID et stockage avancé

11.1 Rappel des configurations

RAID (*Redundant Array of Independent Disks*) combine plusieurs disques pour la performance, la résilience, ou les deux. Les niveaux courants en 2026 :



Comparaison RAID 0 / RAID 5 / RAID 6 : répartition des blocs de données et de parité.

Niveau	Description	Tolérance panne	Usage
RAID 0	Striping pur, performance	Aucune	Caches, scratch — JAMAIS pour données
RAID 1	Mirroring	1 disque	Petits serveurs, simplicité
RAID 5	Striping + parité distribuée	1 disque	NAS, serveurs PME — courant
RAID 6	Striping + double parité	2 disques	Stockage grande capacité
RAID 10	Miroir de stripes	Jusqu'à N/2	Performance + redondance
SHR	Synology Hybrid RAID, taille variable	1 (SHR) ou 2 (SHR-2)	NAS Synology

11.2 La règle d'or RAID : imager AVANT toute chose

Le piège mortel en récupération RAID, c'est la **reconstruction automatique** (rebuild) sur un array dégradé. Quand un disque tombe, beaucoup de contrôleurs RAID matériels proposent (ou lancent automatiquement) une reconstruction sur un disque de remplacement. Le problème : la reconstruction **écrit massivement** sur les disques restants. Si un autre disque était en train de mourir silencieusement, la charge supplémentaire de la reconstruction peut le faire basculer.

Attention — Sur un RAID dégradé contenant des données importantes : **arrêter le serveur, étiqueter physiquement chaque disque avec sa position dans la baie, et imager chaque disque individuellement avant toute autre opération**. La reconstruction se fera plus tard, sur les images, dans un environnement isolé.

11.3 Reconstruction logicielle

Une fois chaque disque imagé en lecture seule, on reconstruit le RAID virtuellement avec des outils comme R-Studio Network, UFS Explorer RAID, ReclaiMe Pro, ou (côté open source) mdadm sous Linux. Le défi est de retrouver les paramètres exacts :

- L'**ordre des disques** dans le stripe.
- La **taille du stripe** (chunk size : 64 Ko, 128 Ko, 256 Ko sont les valeurs courantes).
- Le **schéma de parité** (left-symmetric, left-asymmetric, right-symmetric, right-asymmetric).
- L'**offset** initial (les premiers Mo de chaque disque sont souvent réservés au contrôleur RAID).
- Le **parity delay** sur certaines configurations Dell PERC et HP Smart Array.

Sur les contrôleurs RAID matériels propriétaires (Dell PERC, HP Smart Array, LSI/Avago/Broadcom), des outils comme R-Studio et UFS Explorer Professional reconnaissent automatiquement les métadonnées de configuration. Quand ces métadonnées sont corrompues, on doit deviner les paramètres par analyse entropique.

RETOUR DE LABO — DAFOTEC • RAID 5 Dell PowerEdge, 3 disques en « Foreign » (cas n°2)

Support : RAID 5 / 6 disques de 4 To • **Délai :** 48 heures (astreinte) • **Forfait :** 2 700 € HT

Symptôme. Coupure de courant et surtension. Au redémarrage, le contrôleur PERC H730 signale 3 disques en état « Foreign » et refuse de monter l'array. La reconstruction automatique a été heureusement désactivée par l'administrateur.

Intervention. Étiquetage physique de chaque disque dans sa baie. Clonage forensique de chacun des 6 disques avec ddrescue et write blocker, vers des disques de destination identiques. Reconstruction virtuelle de la parité XOR sans aucune écriture sur les originaux. Identification de l'ordre des disques et du parity delay propre au PERC H730 par analyse entropique.

Résultat. 22 To de données comptables récupérés intégralement. Reprise d'activité du cabinet en moins de 48h.

Cabinet comptable (38 collaborateurs), Lyon — arrêt d'activité évité. Cas publié sur dafotec.fr.

11.4 NAS Synology / QNAP

Les NAS grand public et PME utilisent souvent des FS modernes (Btrfs sur Synology, ZFS sur certains QNAP) avec leurs propres métadonnées de configuration (SHR, SHR-2 chez Synology). Quand un NAS tombe :

- Ne jamais réinitialiser le NAS — la configuration RAID est dans les métadonnées sur les disques.
- Extraire les disques en notant leur ordre d'origine.

- Sous Linux, mdadm --examine sur chaque disque révèle la configuration.
- UFS Explorer Professional et ReclaiMe Pro reconnaissent automatiquement les configurations Synology et QNAP.

NAS et ransomware — Sur les NAS Synology DSM 7 modernes, le système de fichiers Btrfs active par défaut les snapshots. En cas d'attaque ransomware, la procédure type est : 1) clonage forensique des disques, 2) assemblage en lecture seule avec mdadm --assemble --readonly, 3) montage btrfs -o ro,recovery, 4) btrfs subvolume list -s pour identifier les snapshots antérieurs à l'attaque, 5) extraction des données propres depuis ces snapshots. Sur un grand nombre d'attaques eCh0raix, QlockerBunny et DeadBolt, cette procédure permet d'éviter tout paiement de rançon.

11.5 Récupération à partir de chip-off sur NAS

Quand les disques d'un NAS sont eux-mêmes physiquement HS (panne de plusieurs disques après surtension par exemple), il faut combiner les techniques précédentes : récupérer chaque disque individuellement (head swap, PCB swap, imagerie d'urgence si possible), puis reconstruire le RAID virtuellement à partir des images partielles obtenues. Le taux de succès dépend de la combinaison.

11.6 Récupération sur support monolith (microSD, clé USB tout-en-un)

Les **supports monolith** sont des composants où la NAND, le contrôleur et l'interface sont noyés dans une même résine époxy : microSD, clés USB 3.0 tout-en-un, certaines cartes CFast. Quand le composant est physiquement endommagé (contacts oxydés, résine fissurée, support écrasé), on ne peut ni désouder les puces ni accéder au contrôleur par les voies classiques.

La technique de récupération consiste à :

1. Abraser au laser ou chimiquement la résine époxy pour exposer les pistes internes du composant.
2. Identifier au microscope les points de contact correspondant aux broches data de la NAND.
3. Micro-souder des fils de cuivre extrêmement fins (0,02 mm) sur ces points.
4. Connecter à un programmeur NAND universel et procéder à un dump brut comme dans un chip-off classique.
5. Reconstruire logiquement (descrambling, ECC, FTL) comme en 10.3.3.

Cette procédure très technique est documentée publiquement par DAFOTEC sous le nom *Spider Web*, en référence à la toile de fils de cuivre fins qui en résulte sous microscope. Très peu de laboratoires en France maîtrisent cette technique.

RETOUR DE LABO — DAFOTEC • Carte microSD drone DJI Mavic 3 (cas n°6)

Support : microSD 256 Go UHS-II (support monolith) • **Délai :** 4 jours • **Forfait :** 320 € HT

Symptôme. Drone crashé d'environ 40 mètres de hauteur. Carte microSD non reconnue, contacts oxydés visibles à l'œil nu, résine du composant fissurée le long du bord supérieur.

Intervention. Technique Spider Web : abrasion laser de la résine époxy au niveau des broches NAND, identification des points de contact au microscope, micro-soudure de 28 fils de cuivre de 0,02 mm sur les broches data. Dump brut au programmeur NAND, puis reconstruction logique (descrambling, ECC, réassemblage des pages).

Résultat. 240 Go récupérés sur 256 Go — 4h20 de vidéos 4K de repérage architectural. Les 16 Go manquants correspondaient à des secteurs physiquement écrasés à l'impact.

Vidéaste professionnel, Nice — tournage commercial sauvé. Cas publié sur dafotec.fr.

Partie IV

Cas spéciaux

Trois domaines où les techniques générales se heurtent à des contraintes spécifiques : le chiffrement (qui peut transformer un cas trivial en impossible), les supports mobiles (smartphones, Mac modernes), et le contexte judiciaire (où la procédure compte autant que la technique).

PARTIE IV — CAS SPÉCIAUX

Chapitre 12

Chiffrement et récupération

12.1 Une bascule de paradigme

Quand un support n'est pas chiffré, la donnée est lisible par quiconque accède au stockage physique. Quand un support est chiffré, la donnée n'est plus une information ; c'est une suite de bits indistinguable de bruit aléatoire. La récupération devient un problème de cryptanalyse, ce qui veut dire en pratique : **impossible sans la clé**.

12.2 BitLocker (Windows)

BitLocker chiffre les volumes Windows avec AES-128 ou AES-256. La clé maître (FVEK) est protégée par un ou plusieurs **protecteurs** :

- TPM (Trusted Platform Module) : la clé est stockée dans le module de la carte mère, libérée au démarrage si l'état système est conforme.
- Mot de passe utilisateur.
- Clé de récupération à 48 chiffres (sauvegardée dans le compte Microsoft / Azure AD, ou imprimée).
- Clé USB, carte à puce.

Sans aucun protecteur, AES-128 ou AES-256 correctement implémenté résiste à toutes les attaques connues. Renoncer.

Bonne piste systématique : la clé de récupération sauvegardée dans le compte Microsoft. À récupérer via account.microsoft.com ou via l'administrateur AD/Azure en entreprise.

12.3 FileVault (macOS)

FileVault 2 chiffre l'intégralité du volume APFS avec AES-XTS. Sur Mac Apple Silicon (M1 à M4), c'est activé par défaut et géré par la Secure Enclave.

Voies de récupération :

- Mot de passe utilisateur.
- Clé de récupération à 24 caractères (sauvegardée dans iCloud à l'activation, ou notée par l'utilisateur).
- Clé institutionnelle pour les Mac d'entreprise (configurée par le service IT avant déploiement).

Sans aucune de ces voies, le chip-off n'a aucun intérêt : on n'obtient que du chiffré.

12.4 LUKS (Linux)

LUKS (Linux Unified Key Setup) est le standard Linux. Implémenté par cryptsetup. L'en-tête LUKS contient jusqu'à 8 slots de passphrase ; chacun protège une copie chiffrée du master key.

- Avec passphrase connue : cryptsetup open.

- En-tête corrompue mais sauvegarde (cryptsetup luksHeaderBackup) : on restaure.
- Sans rien : Argon2/PBKDF2 + facteur de coût élevé rendent le brute force impraticable sur passphrase moderne.

Conseil de prévention — Sauvegarder l'en-tête LUKS dès l'installation est une bonne pratique. Une corruption des premiers secteurs sans sauvegarde rend le volume définitivement illisible.

12.5 Self-Encrypting Drives (SED, TCG Opal)

Le chiffrement matériel intégré au contrôleur SSD est de plus en plus la norme. Il est :

- Toujours actif (le contrôleur déchiffre avec une clé par défaut si aucun mot de passe n'est défini).
- Activable via BIOS/UEFI (mot de passe ATA) ou logiciel TCG Opal Manager.
- Effaçable instantanément par *crypto erase* — c'est ce qui rend la mise au rebut des SSD sécurisée en quelques secondes.

Plusieurs SSD ont eu des implémentations Opal défaillantes (Crucial MX100/MX200, Samsung 840/850 EVO d'avant firmware EMT02B6Q) qui permettaient de contourner — mais compter là-dessus est jouer au loto.

12.6 Ransomware : ce qui est réellement possible

Quand un poste ou un serveur est touché par un ransomware moderne, les fichiers utilisateurs sont chiffrés avec une clé (typiquement AES) elle-même chiffrée par la clé publique de l'attaquant. Sans la clé privée correspondante, le déchiffrement est mathématiquement impossible.

Voies à examiner systématiquement avant de céder au désespoir :

1. **Decryptor public ?** Le projet *No More Ransom* (nomoreransom.org), porté par Europol, publie des outils gratuits pour les variantes dont les clés ont été saisies ou les failles découvertes. Plus de 200 outils en 2026.
2. **Machine encore allumée ?** Si l'attaque est récente, la clé AES en clair peut être encore en mémoire. Analyse RAM avec Volatility ou DumpIt.
3. **Shadow Copies ?** Sur Windows, vssadmin list shadows peut révéler des Shadow Copies que le ransomware n'a pas réussi à supprimer.
4. **Snapshots Btrfs/ZFS sur NAS ?** La plupart des ransomwares NAS chiffrent les fichiers visibles mais oublient les snapshots en lecture seule. Procédure type au chapitre 11.
5. **Sauvegardes immuables ou air-gappées ?** Question primordiale (chapitre 17).
6. **Faut-il payer ?** Question complexe. 64 % des victimes refusaient en 2024 (DBIR 2025). Payer n'offre aucune garantie de déchiffrement.

Attention — Conserver les fichiers chiffrés même si on ne peut pas les déchiffrer aujourd'hui. Les clés des ransomwares historiques sont régulièrement saisies par les forces de l'ordre (LockBit, Hive, REvil) et publiées des mois ou années après. Stockez les fichiers chiffrés sur un disque hors-ligne ; un jour, vous pourrez peut-être les déchiffrer.

RETOUR DE LABO — DAFOTEC • NAS Synology DS920+ chiffré par ransomware eCh0raix (cas n°4)

Support : NAS RAID 5 / 4 disques de 8 To • **Délai :** 7 jours • **Forfait :** 1 800 € HT

Symptôme. Attaque eCh0raix sur un NAS exposé à Internet. Tous les fichiers utilisateur chiffrés avec extension .encrypt. Deux disques membres du RAID également en erreur côté contrôleur.

Intervention. Clonage forensique des 4 disques avec ddrescue. Assemblage en lecture seule du volume SHR Btrfs via mdadm. Analyse des snapshots Btrfs : identification du dernier snapshot antérieur à l'attaque, daté de la nuit précédente. Extraction du subvolume sain par btrfs send/receive vers stockage propre.

Résultat. 24 To récupérés via le snapshot Btrfs J-1. Aucune rançon payée.

PME e-commerce (12 salariés), Lille — base de données produits intacte. Cas publié sur dafotec.fr.

12.7 Étude de cas — Maersk et NotPetya (juin 2017)

■ Maersk / NotPetya : la sauvegarde sauvée par une panne de courant

Le 27 juin 2017, le géant maritime Maersk est touché par **NotPetya**, malware destructeur déguisé en ransomware, propagé via une mise à jour piégée du logiciel comptable ukrainien M.E.Doc. En 7 minutes, le malware se propage à travers tout le réseau Maersk : 45 000 à 49 000 postes, 4 000 serveurs détruits, dont la totalité des ~150 **contrôleurs de domaine Active Directory**. NotPetya n'est pas réversible : les machines sont mortes.

Maersk a des sauvegardes des serveurs individuels (3 à 7 jours d'âge), mais aucune sauvegarde des contrôleurs de domaine — l'architecture supposait que les 150 contrôleurs se sauvegardaient mutuellement par réplication. Or ils ont tous été détruits simultanément. Sans AD, rien ne peut être restauré.

Salvation : un contrôleur de domaine au Ghana était **hors ligne** au moment de l'attaque, à cause d'une panne de courant locale. Il avait survécu. Maersk l'a fait acheminer physiquement (le réseau étant détruit) à Londres où le centre de récupération avait été monté. Ce contrôleur a servi de base pour reconstruire la totalité de l'infrastructure.

Bilan : 10 jours de paralysie totale, perte estimée 250-300 millions de dollars pour Maersk. Au global, NotPetya a coûté environ 10 milliards de dollars à travers Merck, FedEx/TNT, Mondelez, Saint-Gobain. Sources : Wired *The Untold Story of NotPetya* (2018) ; Control Engineering *Throwback Attack* (2025).

Leçon : les sauvegardes en ligne et synchrones entre elles ne protègent pas contre une attaque qui les détruit toutes en même temps. La survie est venue d'un hasard. Une sauvegarde air-gappée ou immuable aurait évité le hasard.

PARTIE IV — CAS SPÉCIAUX

Chapitre 13

Supports mobiles et Mac Apple Silicon

13.1 Le contexte

Un smartphone moderne contient typiquement plus de données personnelles qu'un ordinateur de bureau. Mais c'est aussi l'un des supports les plus difficiles à récupérer :

- Chiffrement par défaut (iPhone depuis 2010 ; Android 6 depuis 2015 en pratique).
- Stockage eMMC ou UFS monolithique (NAND et contrôleur dans une même puce).
- Liaison forte avec un compte cloud.

13.2 iPhone et iOS

Depuis l'iPhone 5s (2013), la **Secure Enclave** stocke les clés et applique une politique stricte sur le déchiffrement. Toute donnée sur la NAND est chiffrée par une clé liée au passcode et à un UID matériel inscrit dans la Secure Enclave.

- Le chip-off donne du chiffré ininterprétable.
- Les outils forensiques pros (Cellebrite UFED, GrayKey Grayshift, Magnet GrayKey) exploitent des failles non publiques de certaines versions iOS. Fenêtres qui se ferment à chaque mise à jour.
- Pour le particulier : sauvegarde iTunes/Finder ou sauvegarde iCloud.

13.3 Android

Plus hétérogène. Chiffrement par défaut depuis Android 6, basé sur le passcode et un keystore matériel (**TEE**). Android 10+ utilise le chiffrement par fichier.

Outils :

- **Suites forensiques pros** : Cellebrite UFED, MSAB XRY, Oxygen Forensic Detective, Magnet AXIOM.
- **ADB** : sur téléphone vivant et déverrouillé avec débogage USB activé.
- Mode **Download / EDL** sur certaines puces Qualcomm — désormais signé par le fabricant.

Pour un Android verrouillé perdu, la voie la plus praticable reste la **sauvegarde Google** (Photos, Drive, Contacts, Google One backups).

13.4 Smartphones physiquement détruits

Quand le smartphone est physiquement détruit (chute, écrasement, carte mère cassée en deux), des techniques avancées existent mais demandent un laboratoire :

- **Micro-soudure board-level** : réparation des pistes coupées, remplacement de composants défectueux (PMIC, U2).
- **CPU swap mobile** : transplantation du processeur (qui contient la Secure Enclave / TEE et donc les clés de chiffrement) sur une carte mère donneuse vierge, préservant la chaîne

cryptographique. Procédure standardisée dans les laboratoires de niveau labo, documentée publiquement par DAFOTEC.

- **Lecture directe NAND** sur la puce eMMC ou UFS désoudée — mais sans la Secure Enclave, on n'obtient que du chiffré.

RETOUR DE LABO — DAFOTEC • iPhone 15 Pro écrasé par un tracteur (cas n°5)

Support : iPhone 15 Pro • **Délai :** 10 jours • **Forfait :** 380 € HT

Symptôme. iPhone passé sous les roues d'un tracteur agricole. Châssis plié à 90°, carte mère fissurée transversalement en deux, écran pulvérisé. Aucune réponse à l'alimentation.

Intervention. Micro-soudure forensique de la carte mère sous microscope : reconnexion des pistes coupées de part et d'autre de la fissure. Transplantation du processeur Apple A17 Pro (CPU swap mobile, contenant la Secure Enclave et donc les clés FileVault de l'appareil) sur une carte mère donneuse vierge en station BGA. Préservation de la chaîne cryptographique. Extraction de l'image UFS après démarrage en mode DFU.

Résultat. 100 % des contacts, SMS, photos, calendrier et données applicatives (WhatsApp, banque) récupérés.

Agriculteur, Normandie — carnet de contacts professionnel sauvé. Cas publié sur dafotec.fr.

13.5 Mac Apple Silicon : T2 et M1-M4

Sur les Mac Apple Silicon (M1, M2, M3, M4) et les anciens Mac Intel à puce T2 (2018+), le SSD est **soudé à la carte mère** et son contrôleur est intégré au SoC. Trois conséquences :

- Pas de SSD amovible — toute intervention demande d'ouvrir et de travailler sur la carte mère elle-même.
- FileVault actif par défaut, clé liée à la Secure Enclave du SoC.
- Une panne d'alimentation board-level (rails PPBUS_G3H, PP3V3_S5, PP1V8_NAND) suffit à rendre tout l'appareil non démarrable malgré une NAND intacte.

Procédure type pour récupérer un Mac Apple Silicon dont la carte mère est défaillante mais dont l'utilisateur connaît le mot de passe FileVault :

1. Analyse aux schématics et boardview pour identifier les rails d'alimentation morts.
2. Réparation au niveau composant des MOSFET et PMIC grillés.
3. Si la carte mère est trop endommagée pour être réparée, transplantation des composants critiques (SoC, contrôleur SSD soudé, NAND) sur une carte mère donneuse de modèle identique.
4. Lecture du SSD interne via interface DFU matérielle.
5. Déchiffrement par le mot de passe utilisateur.
6. Extraction de l'image sur support neuf.

RETOUR DE LABO — DAFOTEC • MacBook Pro M2, SSD soudé, mise à jour macOS bloquée (cas n°3)

Support : MacBook Pro 14" M2 (2023) • **Délai :** 5 jours • **Forfait :** 480 € HT

Symptôme. MacBook bloqué au logo Apple après une mise à jour macOS 14.4. Démarrage en mode recovery impossible. Aucune lecture par DFU standard. Utilisateur en possession du mot de passe FileVault.

Intervention. Extraction de la carte mère, analyse au boardview. Identification d'un rail d'alimentation défectueux côté SSD soudé. Lecture directe des puces NAND Apple via interface DFU matérielle propriétaire après réparation board-level. Déchiffrement via le mot de passe FileVault fourni par la cliente.

Résultat. 890 Go récupérés sur 1 To — photos Lightroom complet, projets Final Cut Pro intacts, documents professionnels.

Réalisatrice indépendante, Bordeaux — 3 ans de rushes sauvés. Cas publié sur dafotec.fr.

13.6 Le rôle des sauvegardes cloud

Pour les supports mobiles, c'est presque toujours la voie la plus productive. Récupérer depuis iCloud (Photos, contacts, mail, Drive, sauvegardes iOS), Google (Photos, contacts, agenda, Drive, sauvegardes Android), WhatsApp/Signal/Telegram. La majorité des particuliers en perte de données mobile ignore ce qu'ils ont sauvegardé automatiquement.

PARTIE IV — CAS SPÉCIAUX

Chapitre 14

Forensique judiciaire

14.1 La différence fondamentale

La récupération classique a un objectif simple : récupérer ce qui peut l'être. La forensique judiciaire en ajoute un second : **produire un résultat recevable devant un tribunal**. La procédure devient aussi importante que la technique.

- Documentation continue (*chain of custody*).
- Vérification d'intégrité par hash à chaque étape.
- Usage de write blockers.
- Reproductibilité : un autre expert doit pouvoir refaire l'analyse et obtenir les mêmes résultats.
- Outils reconnus et validés.

14.2 ISO 27037 : la norme de référence

La norme **ISO/IEC 27037:2012** définit le cadre international en quatre phases :

1. **Identification** : localiser les supports porteurs de preuves.
2. **Collecte** : prendre possession physique de manière documentée.
3. **Acquisition** : créer une copie forensique vérifiée.
4. **Préservation** : maintenir l'intégrité dans le temps, avec chaîne de custody documentée.

En France, l'expert judiciaire en informatique opère dans le cadre du Code de procédure pénale et doit être inscrit sur la liste des experts près une cour d'appel. Les saisies sont effectuées par la PJ (sous-direction de la lutte contre la cybercriminalité) avec l'appui d'experts.

14.3 Chaîne de custody pas-à-pas concrète

Voici une procédure complète et concrète, telle qu'on peut l'appliquer pour qu'un travail forensique reste recevable :

1. **Documentation à la réception.** Photos haute résolution du support sous tous les angles, sous éclairage uniforme. Notation du fabricant, modèle, numéro de série, capacité indiquée. Pesée si pertinent. État physique général. Tous ces éléments dans un procès-verbal de réception signé par le porteur et le réceptionneur, daté à la minute près.
2. **Étiquetage et scellement.** Apposition d'un sachet scellé numéroté contenant le support. Numéro tracé dans un registre maître. Cellophane ou sachet inviolable préféré.
3. **Conservation.** Stockage dans un coffre ou armoire verrouillée avec accès tracé (badge, registre papier ou les deux).
4. **Préparation de l'acquisition.** Sortie du scellé : vérification que le scellé est intact, photo, notation dans le registre maître de l'opérateur, de la date, de l'heure et de la raison.

5. **Connexion au poste d'analyse.** Toujours via un write blocker matériel (Tableau Forensic Universal Bridge, WiebeTech Forensic UltraDock, Atola Insight). Notation du modèle et numéro de série du write blocker.
6. **Acquisition.** Création de l'image en format E01 ou DD brut avec FTK Imager, dc3dd, ou Atola. Calcul automatique de MD5 + SHA1 (ou SHA256). Notation des hashs dans le rapport.
7. **Vérification croisée.** Calcul d'un hash directement sur la source via le write blocker (lecture seule). Comparaison avec le hash de l'image. Les deux doivent correspondre bit à bit.
8. **Re-scellement.** Remise immédiate de la source dans son sachet, re-scellement, photo, registre.
9. **Analyse.** Tout travail se fait exclusivement sur des copies de l'image (pas sur l'image E01 originale). Chaque outil utilisé est noté avec sa version exacte. Chaque manipulation est journalisée.
10. **Rapport.** Description du support, procédure complète, hashs, outils, méthodologie, conclusions, liste des artefacts produits. Signature de l'expert et date.

Pourquoi c'est crucial — Une chaîne de custody défaillante (scellé brisé non documenté, hash absent ou divergent, écriture inadvertante sur la source, outil non identifié) peut suffire à rendre l'ensemble des conclusions non recevables — peu importe la qualité technique de l'analyse en aval. C'est la dimension la plus souvent sous-estimée par les non-spécialistes.

14.4 Outils forensiques de référence

- **EnCase Forensic** (OpenText) : suite historique.
- **FTK** (AccessData / Exterro). FTK Imager seul est gratuit.
- **X-Ways Forensics** : référence européenne, léger et rapide.
- **Magnet AXIOM** : focus artefacts cloud, mobile et navigateur.
- **Belkasoft X** : très bon sur mobile et messagerie.
- **The Sleuth Kit + Autopsy** : open source, gratuit, largement suffisant pour beaucoup de cas.

14.5 Artefacts Windows à analyser

- **Registre** (NTUSER.DAT, SOFTWARE, SYSTEM, SAM) : config, USB connectés, programmes exécutés (UserAssist, ShellBags, MUICache).
- **Prefetch** : trace des programmes exécutés.
- **ShellBags** : dossiers visualisés dans l'Explorateur.
- **RecycleBin** : fichiers supprimés via la corbeille.
- **$LogFile et $UsnJrnl** : journal NTFS.
- **Event Logs** (.evtx).
- **Browsers** : historique, cookies, cache, téléchargements.

Attention — Ne *jamais* démarrer la machine cible sur son OS d'origine. Tout démarrage modifie des centaines de fichiers (timestamps, logs, registre), ce qui peut suffire à invalider la preuve. Toujours retirer le disque ou démarrer sur un live forensique en lecture seule (CAINE, DEFT, Tsurugi Linux).

Partie V

Pratique

Deux chapitres pour passer de la théorie aux choix concrets : quels outils utiliser dans quelle situation, et quels pièges éviter — avec quatre scénarios pas-à-pas qui couvrent les cas les plus fréquents.

PARTIE V — PRATIQUE

Chapitre 15

Outils 2026 : panorama réaliste

15.1 Méthode

Ce chapitre liste les outils sans donner de « note sur 5 » ou de « taux de récupération » chiffré. Ces classements sont presque toujours : issus de sites affiliés des éditeurs, basés sur des tests non reproductibles, ou copiés d'année en année. Ce qui suit est une description fonctionnelle et un positionnement honnête.

15.2 Outils open source

ddrescue (GNU)

L'outil incontournable pour l'imagerie. Voir chapitre 6.

TestDisk (CGSecurity)

Réparation de tables de partition, récupération de partitions effacées. Pour beaucoup de cas logiques courants, c'est tout ce dont on a besoin.

PhotoRec (CGSecurity)

Carving signature-based. Plus de 480 formats reconnus. Multiplate-forme. Référence open source du carving.

The Sleuth Kit + Autopsy

Suite forensique complète. fls, icat, tsk_recover en CLI, Autopsy en interface web.

extundelete, ext4magic, debugfs

La triade Linux pour ext4.

Outils d'Eric Zimmerman

Suite gratuite pour Windows : MFTECmd, RECmd, LECmd, JLECmd, PECmd, Timeline Explorer. Devenus références du DFIR Windows.

15.3 Outils commerciaux grand public et PME

Disk Drill (CleverFiles)

Windows et macOS. Interface accessible. Version gratuite limitée à 500 Mo.

EaseUS Data Recovery Wizard

Très propre, multi-FS, version gratuite jusqu'à 2 Go.

Recuva (CCleaner)

Gratuit, simple. Adapté aux suppressions accidentelles récentes sur Windows. Limité pour les cas complexes.

Stellar Data Recovery

Gamme complète. Bonne réputation sur Office et multimédia.

15.4 Outils professionnels

R-Studio (R-Tools Technology)

Référence pour les techniciens IT et petits laboratoires. Très bon sur NTFS, ext4, APFS, RAID.

UFS Explorer (SysDev Laboratories)

Excellent sur formats avancés (APFS, ZFS, Btrfs, NAS Synology/QNAP, RAID complexes). Édition Professional très complète. Utilisée dans beaucoup de labos européens.

ReclaiMe et ReclaiMe Pro

Spécialisés dans la reconstruction RAID et les configurations propriétaires (SHR, ZFS, Storage Spaces).

15.5 Outils forensiques judiciaires

EnCase, FTK, X-Ways, Magnet AXIOM, Belkasoft X, Cellebrite UFED, Oxygen Forensic, MSAB XRY. Réservés aux institutions et entreprises spécialisées.

15.6 Plateformes hardware de laboratoire

- **PC-3000** (ACE Lab) : standard de facto. Modules HDD, SSD, Flash, RAID, mobile.
- **DeepSpar / Atola** : alternatives ciblées.

L'équipement complet d'un laboratoire représente plusieurs dizaines de milliers d'euros.

15.7 Matrice de décision

Situation	Premiers outils à essayer
Suppression accidentelle récente sur HDD	TestDisk + PhotoRec (gratuit) ou Disk Drill / EaseUS
Suppression sur SSD (TRIM probable)	Tenter Recuva/EaseUS sans grand espoir ; SSD débranché → labo
Volume devenu RAW (NTFS/exFAT corrompu)	TestDisk pour la partition, R-Studio ou UFS Explorer pour le FS
NAS Synology/QNAP HS	Sortir les disques, UFS Explorer Professional ou ReclaiMe Pro
RAID 5 dégradé	Imager d'abord, puis R-Studio Network ou UFS Explorer RAID
Mac sous FileVault, clé connue	Démarrer en target disk mode, copier ; ou R-Studio for Mac
Mac sous FileVault, clé inconnue	Vérifier iCloud (clé de récupération) ; sinon renoncer
HDD qui claque	Éteindre immédiatement → labo (jamais soi-même)
SSD non détecté	Labo (JTAG / chip-off)
Mac Apple Silicon non démarrable, FileVault connu	Labo (board-level + lecture DFU)
Cas judiciaire (preuve à produire)	FTK Imager (gratuit) + Autopsy, ou suite pro (X-Ways, EnCase, AXIOM)
Téléphone Android verrouillé	Sauvegarde Google ; pour le forensique : Cellebrite, MSAB
iPhone verrouillé	Sauvegarde iCloud ; pour le forensique : GrayKey (modèles vulnérables)
NAS Synology chiffré par ransomware	Clonage + analyse snapshots Btrfs (chap. 11)

PARTIE V — PRATIQUE

Chapitre 16

Pièges mortels et scénarios pas-à-pas

16.1 Les sept erreurs qui tuent les données

1. **Installer un logiciel de récupération sur le support source.** L'installation écrit là où sont les fichiers supprimés.
2. **Récupérer les fichiers sur le support source.** Variante tout aussi catastrophique.
3. **Laisser un SSD sous tension après l'incident.** TRIM et GC continuent.
4. **Accepter la réparation automatique de Windows.** chkdsk /f, autorepair sur un FS corrompu : Windows écrit, déplace, supprime activement.
5. **Ouvrir un HDD hors salle blanche.** Voir chapitre 9.
6. **Dessouder une puce NAND avec un fer à souder.** Sans station de rework calibrée, la puce est détruite.
7. **Conserver les sauvegardes dans le même environnement que la production.** Cas Code Spaces (ci-dessous). Le ransomware moderne cible les sauvegardes accessibles.

16.2 Étude de cas — Code Spaces (juin 2014)

■ Code Spaces : 12 heures de l'entreprise à la disparition

Code Spaces était une plateforme de code hosting (Subversion et Git) avec 7 ans d'historique, basée au Royaume-Uni, intégralement hébergée sur AWS.

Le 17 juin 2014, l'entreprise subit une attaque DDoS suivie d'un message extorquant un paiement, laissé directement dans la console EC2. L'attaquant avait obtenu l'accès au panneau AWS — par compromission de credentials, sans MFA activé.

Code Spaces refuse de payer et tente de reprendre le contrôle. Mais l'attaquant avait déjà créé plusieurs comptes en arrière-plan. Réalisant que Code Spaces essayait de reprendre la main, il lance une suppression méthodique : **EBS snapshots, S3 buckets, AMI, instances EC2, instances de stockage**.

Le point critique : *les sauvegardes étaient dans le même compte AWS que la production*. Une fois l'accès obtenu, l'attaquant a pu tout supprimer simultanément.

Le 18 juin 2014 — 12 heures après le début de l'attaque — Code Spaces annonce la cessation définitive d'activité. Sources : Threatpost (juin 2014) ; InfoWorld *Murder in the Amazon cloud* (2014) ; analyse Wiz *breaches.cloud* (2023).

Leçons : (1) ne jamais stocker les sauvegardes dans le même compte/domaine que la production ; (2) MFA obligatoire sur tout compte de gestion cloud ; (3) principle of least privilege ; (4) avoir un plan de réponse à incident testé.

16.3 Quatre scénarios pas-à-pas

Scénario A — Clé USB exFAT formatée par erreur

Symptômes : la clé apparaît vide après un formatage rapide déclenché par erreur. L'utilisateur réalise immédiatement.

Diagnostic : logique. Le formatage rapide a réécrit la table FAT et le boot sector, mais pas les clusters de données. Les fichiers sont là, leurs entrées de répertoire aussi (avec première lettre potentiellement perdue).

Chemin recommandé :

1. Débrancher immédiatement la clé.
2. Sur un autre poste, copier l'image de la clé : sudo ddrescue -f -n -d /dev/sdX cle.img cle.map.
3. Travailler sur l'image. Lancer TestDisk dessus pour récupérer la table : testdisk cle.img.
4. Si TestDisk ne reconstruit pas le FS, lancer PhotoRec sur l'image pour du carving signature : photorec cle.img.
5. Récupérer dans un dossier de destination **sur un autre support**.

Issue typique : récupération complète, avec noms souvent intacts.

Scénario B — SSD NVMe, suppression de fichier critique 30 minutes plus tôt

Symptômes : un répertoire entier a été supprimé sur le SSD interne. TRIM est actif par défaut (Windows 10+). La machine est encore allumée et continue d'être utilisée.

Diagnostic : logique sur SSD avec TRIM. Fenêtre presque fermée — chaque minute compte.

Chemin recommandé :

1. **Éteindre immédiatement la machine** (bouton physique, pas « arrêter » qui peut lancer des opérations de fin).
2. Démonter le SSD. Si c'est un SSD soudé (laptop ultrabook, Mac), ne pas rallumer — passer en labo.
3. Pour un SSD démontable : connecter sur un autre poste via un adaptateur SATA-USB ou NVMe-USB **sans monter le système de fichiers en écriture**. Sous Linux : sudo blockdev --setro /dev/sdX avant tout.
4. Imager : sudo ddrescue -f -n -d /dev/sdX ssd.img ssd.map.
5. Sur l'image, tenter une récupération logique avec R-Studio ou TestDisk. Les chances dépendent fortement du SSD modèle et de ce que le GC a fait pendant l'intervalle.

Issue typique : aléatoire. Si TRIM a été transmis et que le GC est passé, peu ou rien. Si la machine a peu travaillé après suppression et que le GC ne s'est pas activé, une partie significative peut être récupérée. Sur SSD NVMe Samsung 980 Pro ou WD SN850 en bonne santé, ne pas être optimiste.

Scénario C — RAID 5 dégradé après mauvaise manipulation

Symptômes : sur un serveur Dell PowerEdge avec 5 disques de 4 To en RAID 5, un disque a affiché « failed » la semaine dernière. L'admin a remplacé un disque (peut-être le mauvais) et lancé une reconstruction. La reconstruction a planté à mi-chemin et le contrôleur affiche maintenant deux disques « foreign ».

Diagnostic : RAID 5 en danger maximal. Une mauvaise intervention peut avoir écrasé partiellement la parité ou les données. C'est typiquement le cas labo.

Chemin recommandé :

1. **Arrêter immédiatement le serveur**. Ne plus lancer aucun rebuild.
2. Étiqueter physiquement chaque disque : position dans la baie (1, 2, 3, 4, 5), modèle, numéro de série, date.
3. Sortir les disques et les imager **individuellement** sur un poste séparé avec write blockers : sudo ddrescue sur chaque, vers des fichiers nommés disk1.img, disk2.img, etc.
4. Travailler sur les images uniquement.
5. Soit en interne avec R-Studio Network / UFS Explorer Professional, soit en faisant appel à un laboratoire spécialisé. Pour ce type de cas, l'intervention pro est généralement préférable.

Issue typique : si on n'a pas lancé une deuxième reconstruction par-dessus, récupérable dans la majorité des cas. Si on a écrasé des données par un rebuild partiel, plus dur.

Scénario D — NAS Synology chiffré par ransomware

Symptômes : tous les fichiers du NAS apparaissent avec une extension étrangère (.encrypt, .lockbit, etc.). Un fichier README ou HOWTODECRYPT est présent à la racine. Le NAS fonctionne mais les fichiers sont inutilisables.

Diagnostic : ransomware NAS (eCh0raix, QlockerBunny, DeadBolt et leurs variantes). Les snapshots Btrfs sont probablement intacts si le NAS tournait en DSM 7+.

Chemin recommandé :

1. **Isoler le NAS du réseau immédiatement** (débrancher câble Ethernet). Ne pas l'éteindre brutalement non plus, faire un arrêt normal.
2. Sortir les disques en notant l'ordre (numéro de baie).
3. Connecter les disques sur un poste Linux dédié, isolé d'Internet.
4. Assembler le RAID en lecture seule : sudo mdadm --assemble --readonly /dev/md0 /dev/sd[abcd]3.
5. Monter Btrfs en recovery : sudo mount -t btrfs -o ro,recovery /dev/md0 /mnt/nas.
6. Lister les snapshots : sudo btrfs subvolume list -s /mnt/nas.
7. Identifier le snapshot le plus récent **antérieur** à l'attaque (généralement J-1 ou J-2).
8. Extraire les fichiers depuis ce snapshot sur un stockage neuf.
9. Restaurer le NAS sur un OS neuf et changer tous les mots de passe.

Issue typique : récupération souvent à 100 %, sans paiement de rançon, dans la majorité des cas où les snapshots étaient configurés. Sinon, vérifier nomoreransom.org.

16.4 Quand savoir s'arrêter

Quatre signes : support physiquement détérioré ; plusieurs tentatives infructueuses ; enjeu supérieur au coût pro ; enjeu judiciaire. Dans ces cas, passer la main.

Partie VI

Prévention

La meilleure récupération est celle qu'on n'a jamais à faire. Deux chapitres pour fermer le cercle : les stratégies de sauvegarde modernes, et un point honnête sur ce qui reste définitivement hors d'atteinte de la récupération en 2026.

PARTIE VI — PRÉVENTION

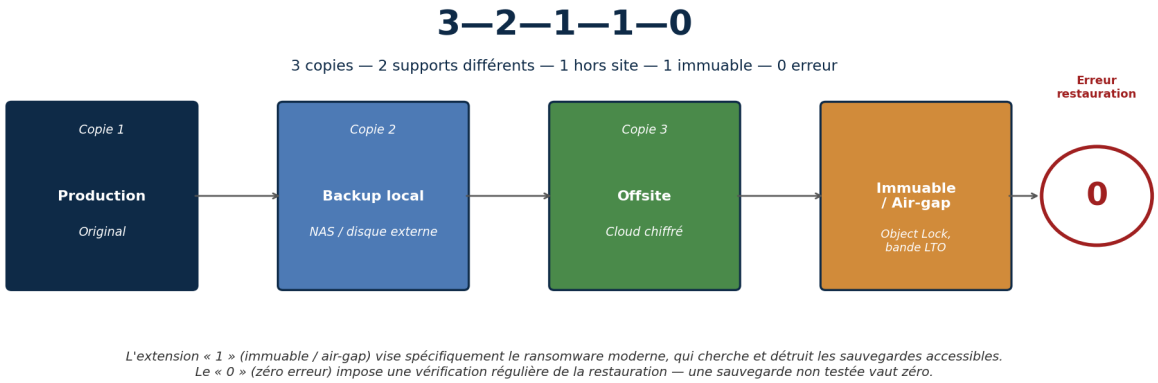
Chapitre 17

Stratégies de sauvegarde modernes

17.1 La règle 3-2-1 et son extension

La **règle 3-2-1** a été formulée en 2005 par Peter Krogh, photographe, dans *The DAM Book*. Elle se résume à : **3** copies, **2** supports différents, **1** hors site.

Vingt ans plus tard, l'omniprésence du ransomware a poussé Veeam à proposer une extension **3-2-1-1-0** : **+1** copie immuable ou air-gappée, **+0** erreur de restauration (testée régulièrement).



La règle 3-2-1-1-0 — quatre copies, une immuable, zéro erreur de restauration.

Sur l'origine — La règle 3-2-1-1-0 est marketing Veeam, pas un standard ANSSI ou NIST. Cela ne lui enlève rien sur le fond : l'immutabilité et l'air-gap sont devenues incontournables face au ransomware moderne. Les principes sont largement repris (Object First, Wasabi, Backblaze B2 avec Object Lock, Azure Blob immutability, Synology SnapLock).

17.2 Mettre en œuvre l'immutabilité

- **Object Lock S3** (AWS, Backblaze B2, Wasabi, MinIO). Mode *compliance* ou *governance*.
- **Azure Blob immutability** et Google Cloud Storage retention policies.
- **Hardened Linux Repository** avec attribut chattr +i et SSH désactivé pour root.
- **WORM** sur bandes ou disques optiques.
- **Snapshots NAS** immuables : Synology SnapLock, QNAP WORM.

17.3 L'air-gap

Un support **air-gappé** est physiquement déconnecté du réseau pendant la majorité du temps. Variantes :

- **Bande LTO** sortie du robot et stockée dans un coffre.
- **Disque USB** connecté uniquement pour la sauvegarde, puis rangé.
- **Rotation de plusieurs disques externes** avec un stockage hors site rotatif.

17.4 La vérification de restauration

Le **0** de 3-2-1-1-0 est le plus négligé. Beaucoup d'organisations ont des sauvegardes qui n'ont jamais été testées. Causes fréquentes d'échec à la restauration :

- Corruption silencieuse (bit rot non détecté).
- Chaîne incrémentale cassée.
- Agent planté silencieusement il y a des mois.
- Application qui ne démarre pas depuis la sauvegarde (dépendance, version, base incohérente).

Bonne pratique : test de restauration **trimestriel** minimum, **mensuel** pour les systèmes critiques. Documenter chaque test.

17.5 Pour le particulier

1. Disque externe à 50-100 euros pour Time Machine / File History.
2. Cloud personnel : iCloud, Google One, Dropbox, OneDrive, Backblaze Personal Backup.
3. Pour les fichiers vraiment irremplaçables, troisième copie sur clé USB stockée chez un proche.
4. Test annuel : essayer de restaurer un fichier au hasard depuis chacune des trois copies.

17.6 Pour les PME

- Sauvegarde quotidienne automatique (Veeam, Acronis, Datto, Synology Active Backup).
- Au moins une copie en cloud immuable.
- Au moins une copie air-gappée hebdomadaire.
- MFA obligatoire sur tous les comptes d'admin.
- Test de restauration mensuel documenté.
- Plan de reprise écrit : qui fait quoi, dans quel ordre, avec quels contacts.
- Exercice annuel : incident fictif, voir si le plan tient.

PARTIE VI — PRÉVENTION

Chapitre 18

Limites actuelles en 2026

18.1 Ce qui est définitivement perdu

1. **SSD avec TRIM passé et GC effectuée.** Les cellules sont à leur état neutre. Aucune technique ne récupère.
2. **Données chiffrées par AES-256 sans la clé.** Mathématiquement irréalisable avec les ordinateurs classiques. L'ordinateur quantique pourrait casser AES-128 par Grover mais pas AES-256, et n'existe pas à l'échelle utile en 2026.
3. **Plateaux HDD avec la couche magnétique arrachée.** L'information était dans le métal.
4. **Fichiers chiffrés par ransomware moderne sans la clé et sans erreur d'implémentation.**
5. **RAID 5 avec plus d'un disque HS, RAID 6 avec plus de deux.** La parité ne suffit plus.
6. **Données écrasées par réécriture complète.** Le mythe de la rémanence magnétique est démenti pour les disques modernes : un seul passage de zéros sur un HDD moderne rend la donnée irrécupérable.

18.2 Ce qui devient difficile

- **Récupération mobile** : Secure Enclave, TEE, chiffrement par défaut ferment les portes. Cellebrite et GrayKey exploitent des failles qui se ferment à chaque mise à jour.
- **SSD classique** : TRIM fiable, chiffrement matériel généralisé, fenêtre raccourcie.
- **Cloud** : suppression définitive côté provider est de plus en plus rigide.

18.3 Le message final de ce chapitre

La récupération de données est une discipline réelle, techniquement complexe, qui a fait d'énormes progrès mais se heurte à des limites physiques et mathématiques de plus en plus serrées. Les méthodes des chapitres 6 à 11 fonctionnent dans une majorité de cas, mais dépendent presque toujours du temps qui s'écoule entre l'incident et la première bonne décision.

La meilleure stratégie reste, sans surprise, de ne pas avoir à récupérer : prévention, sauvegarde réelle testée, discipline opérationnelle quand quelque chose tourne mal. Le chapitre 17 est, en pratique, le plus utile du livre.

Partie VII

Horizon

Un chapitre prospectif. Où va la discipline dans les cinq à dix années qui viennent ? Quelles technologies de stockage vont la remodeler ? Quelles approches émergentes — IA, post-quantique — vont changer le terrain ? Sans promesses, sans prédictions péremptoires : des tendances qu'on voit déjà se dessiner.

PARTIE VII — HORIZON

Chapitre 19

Horizon 2030 : où va la discipline

19.1 Côté supports : densité, complexité

PLC NAND et au-delà

Les premières mémoires **PLC** (5 bits par cellule, 32 niveaux de tension) ont été annoncées par Solidigm et Kioxia entre 2023 et 2025. Commercialisation progressive sur 2026-2028 pour les SSD de très grande capacité (32 To+ consumer). Les conséquences pour la récupération :

- Marges entre niveaux de tension encore plus étroites — sous les 100 mV.
- Endurance théorique en chute libre (probablement moins de 150 cycles P/E par cellule). Compensé par des contrôleurs très sophistiqués (gestion fine des températures, retention monitoring, refresh automatique des cellules).
- Lecture brute par chip-off plus difficile : il faut un VNR ultra-précis, des lectures multiples, et reconstruire un pipeline ECC LDPC encore plus lourd.
- Conséquence pratique : le chip-off sur PLC sera très probablement réservé aux laboratoires de haut niveau ; la voie JTAG/ISP via un contrôleur vivant restera la principale option.

HAMR à grande échelle

Seagate a commencé à commercialiser le HAMR sur ses Mozaic 3+ (30 To et plus) en 2024. Toshiba et Western Digital suivront. À l'horizon 2030, les disques durs grand public 24 et 30 To seront en HAMR. Implications :

- Densité linéaire encore plus élevée (au-delà de 1,4 To/plateau).
- Têtes plus complexes (laser intégré, écriture à 450 °C ponctuel).
- Service Area encore plus critique — la calibration laser/têtes/plateaux est sensible.
- Pour la récupération : pas de changement fondamental dans la méthode (head swap, PCB swap restent applicables), mais les marges techniques se resserrent. Les laboratoires devront mettre à jour leur stock de donneurs et leurs procédures spécifiques au HAMR.

Stockage ADN, holographique, optique 5D

Trois technologies de stockage *archival* sont en R&D; depuis le milieu des années 2010. Aucune n'a passé le stade commercial grand public en 2026, mais les promesses sont réelles :

- **Stockage ADN.** Microsoft, Twist Bioscience, Catalog. Encode des données dans des séquences d'ADN synthétique. Densité théorique de l'ordre du pétaoctet par gramme, durée de vie de plusieurs milliers d'années. Latence et coût encore prohibitifs pour autre chose que l'archivage très long terme.
- **Stockage holographique** (HVD). Plusieurs fois annoncé comme prêt à la commercialisation depuis 2008. Toujours pas généralisé en 2026.
- **Optique 5D / Superman memory crystal** (Université de Southampton). Verre nanostructuré par laser femtoseconde. Capacité expérimentale de 360 To sur un disque, durée de vie estimée à

13,8 milliards d'années.

Pour le récupérateur de données : ces technologies poseront, quand elles arriveront, des problèmes radicalement nouveaux. Lire une donnée ADN dans 50 ans sans le séquenceur original ? Ce n'est plus le même métier. À ce stade, il est trop tôt pour que ces sujets soient autre chose que de la prospective.

19.2 Côté méthodes : IA et automatisation

Carving assisté par IA

Plusieurs éditeurs forensiques ont annoncé des modules d'apprentissage automatique entre 2023 et 2025 :

- **Magnet AXIOM AI** (depuis 2024) : classification automatique d'images potentiellement illégales, détection de visages, transcription audio.
- **Belkasoft X AI** (depuis 2024) : modules de réassemblage de fragments d'images carving, détection de contenu généré par IA.
- **Cellebrite AI Reveal** (annoncé 2025) : résumé automatique de conversations dans les extractions de smartphones.

Promesses réalistes : oui, ces approches accélèrent la classification post-extraction sur de gros volumes. Limites réelles : aucune ne fait de miracle au niveau du carving low-level (récupérer des fichiers fragmentés à partir de NAND brute reste un problème combinatoire dur). L'IA aide en aval, pas en amont.

Reconstruction de FTL assistée par ML

Quelques publications académiques (USENIX, FAST 2023-2025) explorent l'usage de réseaux de neurones pour identifier le polynôme de scrambling et le pipeline ECC d'un contrôleur SSD à partir de signatures sur la NAND brute. Encore expérimental ; à surveiller à 3-5 ans.

19.3 Côté cryptographie : post-quantique

Le NIST a finalisé en 2024 les premières standardisations post-quantiques (CRYSTALS-Kyber pour l'échange de clés, CRYSTALS-Dilithium pour la signature, SPHINCS+ pour le hachage). Le déploiement à grande échelle dans le stockage prendra des années. Implications pour la récupération :

- AES-256 reste robuste contre Grover (réduit la sécurité effective de 256 à 128 bits, ce qui reste irrésoluble). AES-128 deviendra théoriquement cassable mais pas en pratique avant longtemps.
- Les remplacements post-quantiques pour le chiffrement matériel (TCG Opal v2.x avec algo post-quantique) arriveront probablement à partir de 2028-2030.
- Des erreurs d'implémentation dans ces nouveaux algorithmes — comme cela s'est produit avec certaines premières implémentations Opal — rouvriront temporairement des fenêtres de récupération inattendues. Surveiller les avis CVE/CERT-FR.

19.4 Côté juridique et réglementaire

- **NIS2** (Network and Information Security Directive 2, UE) impose à partir d'octobre 2024 des obligations renforcées de gestion d'incident, de sauvegarde et de continuité d'activité. La récupération devient un point réglementaire.

- **DORA** (Digital Operational Resilience Act) pour le secteur financier européen, applicable depuis janvier 2025. Exigences strictes sur les tests de reprise après sinistre.
- **RGPD** : la jurisprudence sur la conservation des copies de récupération s'affine. Les laboratoires sérieux ont contractualisé la destruction des copies temporaires après restitution au client.

19.5 Côté économique

Trois tendances :

- La **tarification publique** s'impose comme norme — il y a quinze ans, presque aucun laboratoire ne publiait ses tarifs. En 2026, DAFOTEC publie une grille complète, et plusieurs laboratoires français suivent. La pression d'opacité commerciale recule.
- Le **paiement au résultat** devient standard. Acceptation par le marché qu'un client ne paie pas si on n'a rien récupéré.
- La **validation avant paiement** (VeriFiles chez DAFOTEC, équivalents chez d'autres labos) devient une attente client de plus en plus explicite.

19.6 Côté formation

La récupération de données reste un métier sans cursus diplômant. La formation se fait par apprentissage en laboratoire et par certifications éditeurs (ACE Lab Certified, EnCase Certified Examiner, GCFE, CFCE). À l'horizon 2030, on peut espérer voir émerger en France des modules dédiés dans les masters de cybersécurité — quelques universités l'ont expérimenté depuis 2023 (M2 Cyber à Lille, à Rennes, à Compiègne, à Lyon).

19.7 Le métier ne disparaît pas

Une crainte récurrente : avec le cloud, les sauvegardes généralisées et le chiffrement par défaut, la récupération de données est-elle un métier d'avenir ou un métier en sursis ?

Trois éléments convergent pour dire que le métier ne disparaît pas :

1. Le volume total de stockage produit dans le monde croît exponentiellement. Même si une part de plus en plus grande est chiffrée ou sauvegardée, le volume résiduel non protégé augmente en valeur absolue.
2. Les pannes matérielles restent inéluctables (AFR HDD ~1,3 % par an, durée de vie SSD finie). Les volumes croissent, donc les besoins en récupération aussi.
3. Les exigences réglementaires (NIS2, DORA, ISO 27001, RGPD) imposent des analyses forensiques et des récupérations documentées de plus en plus rigoureuses. Le métier monte en exigence procédurale.

Ce qui change : le métier devient plus technique (plus de physique, plus d'électronique avancée, plus d'ingénierie inverse), plus normé (chaîne de custody, conformité), et plus concentré (les laboratoires capables d'aller au bout des cas modernes ne sont pas légion). La discipline ne disparaît pas. Elle se professionnalise.

Annexes

Référence rapide

Cinq annexes : commandes de référence et scripts Python utiles, glossaire des termes techniques, bibliographie complète des sources publiques consultées, page « À propos de DAFOTEC », et index thématique.

ANNEXES

Chapitre A

Commandes et scripts de référence

A.1 Identification du support

```
# Linux
$ lsblk -o NAME,SIZE,MODEL,SERIAL,TRAN
$ sudo hdparm -I /dev/sdX
$ sudo smartctl -a /dev/sdX

# macOS
$ diskutil list
$ diskutil info /dev/diskN

# Windows (PowerShell)
PS> Get-PhysicalDisk
PS> Get-Disk | Format-List
```

A.2 Imagerie ddrescue

```
# Première passe rapide
$ sudo ddrescue -f -n -d /dev/sdX image.img image.map

# Deuxième passe avec retry
$ sudo ddrescue -f -d -r3 /dev/sdX image.img image.map

# Passe inverse pour cas sévères
$ sudo ddrescue -f -d -R -r3 /dev/sdX image.img image.map

# Statistiques
$ ddrescuelog -t image.map
```

A.3 Monter une image en lecture seule

```
$ sudo losetup --read-only --find --show image.img
/dev/loop0
$ sudo blkid /dev/loop0

# Si table de partition :
$ sudo partx --show /dev/loop0
$ sudo partx --add /dev/loop0

# Monter selon le FS
$ sudo mount -o ro,noload /dev/loop0p1 /mnt/recup # ext4
$ sudo mount -t ntfs-3g -o ro,norecover /dev/loop0p1 /mnt/recup
$ sudo mount -o ro /dev/loop0p1 /mnt/recup # FAT/exFAT
```

A.4 Hash d'intégrité

```
$ sha256sum image.img > image.img.sha256
$ md5sum image.img > image.img.md5
$ sha256sum -c image.img.sha256

# Sur très gros fichiers, BLAKE3 plus rapide :
$ b3sum image.img
```

A.5 Analyse NTFS

```
# Sleuth Kit
$ fls -r -p image.img
$ icat image.img 12345 > out.bin

# Outils Zimmerman (Windows)
PS> MFTECmd.exe -f C:\Image\$MFT --csv .\out --csvf mft.csv
PS> LogFileParser.exe -f C:\Image\$LogFile -o logfile.csv
PS> UsnJrnl2Csv.exe -f C:\Image\$J -o usnjrnl.csv
```

A.6 Analyse ext4

```
$ sudo extundelete --restore-file 'path/file' /dev/sdb1
$ sudo extundelete --restore-all /dev/sdb1

$ sudo debugfs /dev/sdb1
debugfs: lsdel
debugfs: stat <12345>
debugfs: dump <12345> /tmp/out
```

A.7 RAID Linux (mdadm)

```
$ sudo mdadm --examine /dev/sd[a-d]1
$ sudo mdadm --assemble /dev/md0 /dev/sd[a-d]1
$ sudo mdadm --assemble --force --run /dev/md0 /dev/sd[a-d]1
$ sudo mdadm --detail /dev/md0
$ cat /proc/mdstat
```

A.8 Btrfs et snapshots (NAS)

```
$ sudo mount -t btrfs -o ro,recovery /dev/md0 /mnt/nas
$ sudo btrfs subvolume list -s /mnt/nas
$ sudo btrfs send /mnt/nas/.snapshots/123 \
| sudo btrfs receive /restoration
```

A.9 Vérification TRIM

```
# Windows
C:\> fsutil behavior query DisableDeleteNotify

# Linux
$ cat /sys/block/sdX/queue/discard_max_bytes
$ systemctl status fstrim.timer

# macOS
$ system_profiler SPSerialATADataType | grep -i 'TRIM Support'
```

A.10 Capture RAM (forensique live)

```
# Windows : DumpIt (MoonSols/Comae)
C:\> DumpIt.exe

# Linux : LiME ou AVML
$ sudo insmod lime.ko 'path=/tmp/mem.lime format=lime'

# Analyse Volatility 3
$ vol -f memory.dump windows.info
$ vol -f memory.dump windows.pslist
$ vol -f memory.dump windows.netscan
```


A.11 Script Python : parser de mapfile ddrescue

Petit utilitaire qui parse le mapfile d'une session ddrescue et affiche les statistiques par catégorie de blocs (rescued, non-tried, non-trimmed, non-scraped, slow, bad-sector) :

```
#!/usr/bin/env python3
"""parse_ddrescue_mapfile.py - Statistiques d'un mapfile ddrescue."""
import sys
from collections import Counter

STATUS_LABELS = {
'+': 'rescued',
'?': 'non-tried',
'*': 'non-trimmed',
'/': 'non-scraped',
'-': 'bad-sector',
'F': 'finished',
'L': 'slow',
}

def parse(path):
totals = Counter()
with open(path) as f:
for line in f:
line = line.strip()
if not line or line.startswith('#'):
continue
parts = line.split()
if len(parts) < 3 or parts[2] not in STATUS_LABELS:
continue
size = int(parts[1], 16)
totals[parts[2]] += size
return totals

if __name__ == '__main__':
totals = parse(sys.argv[1])
grand = sum(totals.values())
print(f'Total: {grand/1e9:.2f} GB')
for status, size in totals.most_common():
label = STATUS_LABELS.get(status, status)
pct = size / grand * 100 if grand else 0
print(f' {label:<14} {size/1e9:>8.2f} GB ({pct:>5.2f} %)')
```

Usage : python3 parse_ddrescue_mapfile.py image.map. Utile pour décider s'il faut lancer une passe supplémentaire (si beaucoup de *non-scraped*) ou si le support est sans espoir (beaucoup de *bad-sector*).

A.12 Script Python : extraction d'entrées MFT supprimées

Petit parser pédagogique qui lit un fichier $MFT extrait et liste les entrées marquées comme supprimées avec leur nom de fichier issu de l'attribut $FILE_NAME :

```
#!/usr/bin/env python3
"""parse_mft_deleted.py - Liste les entrees MFT supprimees."""
import sys, struct

RECORD_SIZE = 1024
MFT_RECORD_IN_USE = 0x01

def parse_mft(path):
deleted = []
with open(path, 'rb') as f:
```



```
record_idx = 0
while True:
data = f.read(RECORD_SIZE)
if len(data) < RECORD_SIZE:
break
if data[:4] != b'FILE':
record_idx += 1
continue
flags = struct.unpack('<H', data[22:24])[0]
if not (flags & MFT_RECORD_IN_USE):
# Supprime - chercher l'attribut FILE_NAME (type 0x30)
name = find_file_name(data)
if name:
deleted.append((record_idx, name))
record_idx += 1
return deleted

def find_file_name(record):
# Offset du premier attribut
attr_offset = struct.unpack('<H', record[20:22])[0]
while attr_offset < len(record) - 8:
attr_type = struct.unpack('<I', record[attr_offset:attr_offset+4])[0]
if attr_type == 0xFFFFFFFF:
return None
attr_len = struct.unpack('<I', record[attr_offset+4:attr_offset+8])[0]
if attr_len == 0:
return None
if attr_type == 0x30: # FILE_NAME
content_offset = struct.unpack('<H', record[attr_offset+20:attr_offset+22])[0]
base = attr_offset + content_offset
name_len = record[base + 64]
try:
return record[base+66:base+66+name_len*2].decode('utf-16-le')
except UnicodeDecodeError:
return None
attr_offset += attr_len
return None

if __name__ == '__main__':
for idx, name in parse_mft(sys.argv[1]):
print(f'{idx:>8} {name}')
```

Avertissement — Ces scripts sont pédagogiques et minimalistes. Pour un usage sérieux, préférer MFTECmd (Zimmerman) côté NTFS et la suite Sleuth Kit côté générique. Les scripts ci-dessus servent à comprendre la structure, pas à remplacer les outils éprouvés.

ANNEXES

Chapitre B

Glossaire

AES — Advanced Encryption Standard. Algorithme de chiffrement symétrique standardisé NIST en 2001. AES-128 et AES-256 résistent à toutes les attaques connues avec les moyens classiques actuels.

AFR — Annualized Failure Rate. Taux de panne annualisé d'un parc de disques.

Air-gap — Isolation physique d'un système ou support du réseau.

APFS — Apple File System (2017). Copy-on-write, snapshots, support FileVault natif.

BGA — Ball Grid Array. Boîtier avec matrice de billes de soudure sous le composant, courant pour les puces NAND.

Btrfs — B-tree file system Linux. Copy-on-write avec snapshots et checksums.

Carving — Reconstruction de fichiers à partir de signatures binaires dans les données brutes, sans utiliser les structures du FS.

Chain of custody — Documentation continue de la prise en charge et de chaque manipulation d'une preuve numérique.

Charge trap (CTF) — Architecture de cellule NAND moderne où la charge est piégée dans un isolant, plus robuste que la grille flottante. Adoptée massivement depuis 2017.

Chip-off — Désoudage physique d'une puce NAND pour la lire indépendamment de son contrôleur.

CMR — Conventional Magnetic Recording. Mode HDD avec pistes non-recouvrantes.

Copy-on-write — Toute modification écrit ailleurs et met à jour les pointeurs. Utilisé par APFS, Btrfs, ZFS.

CPU Swap mobile — Transplantation du processeur d'un smartphone sur une carte mère donneuse, préservant la Secure Enclave / TEE. Technique documentée publiquement par DAFOTEC.

DBIR — Data Breach Investigations Report. Rapport annuel Verizon depuis 2008.

ddrescue — GNU ddrescue. Outil d'imagerie bit-à-bit tolérant aux erreurs.

DRAT / DZAT — Deterministic Read After Trim / Deterministic Zero After Trim. Garantis SSD.

ECC — Error-Correcting Code. Codes correcteurs appliqués par le contrôleur SSD à chaque page NAND.

eMMC — embedded MultiMediaCard. Mémoire flash avec contrôleur intégré, format compact pour smartphones bas/moyen de gamme.

ext4 — Système de fichiers Linux par défaut depuis 2008.

FileVault — Chiffrement de volume macOS depuis Mac OS X 10.3, puis FileVault 2 depuis 10.7. Géré par la Secure Enclave sur les Mac Apple Silicon.

FTL — Flash Translation Layer. Couche dans le contrôleur SSD qui mappe LBA logiques aux pages physiques NAND.

Garbage collection (GC) — Processus en arrière-plan du contrôleur SSD qui efface physiquement les blocs marqués libres.

Greffe HSA — Head Stack Assembly transplant. Transplantation du bloc complet de têtes de lecture depuis un disque dur donneur jumeau vers un disque receveur, avec alignement micrométrique inférieur à 0,3 µm.

HAMR — Heat-Assisted Magnetic Recording. Technologie HDD qui chauffe la couche magnétique par laser pendant l'écriture. Commercialisée depuis 2024 sur les très gros disques.

HDD — Hard Disk Drive. Disque dur magnétique mécanique.

Imagerie — Création d'une copie bit-à-bit d'un support vers un fichier image.

ISO 14644-1 — Norme internationale des classes de salle blanche par concentration de particules.

ISO 27037 — Norme internationale pour la collecte et la préservation de preuves numériques.

JTAG / ISP — Protocole de débogage interne exposé par les contrôleurs SSD. Exploité en récupération non destructive.

LBA — Logical Block Address. Adresse logique exposée par l'interface SATA/NVMe.

LDPC — Low-Density Parity-Check. Code correcteur d'erreurs utilisé par les contrôleurs SSD modernes, succédant aux codes BCH classiques.

LUKS — Linux Unified Key Setup. Standard de chiffrement de volume Linux.

Mapfile — Fichier de carte utilisé par ddrescue.

MFT — Master File Table. Structure centrale de NTFS.

NAND flash — Mémoire à grille flottante ou charge trap, technologie sous tous les SSD, eMMC, UFS, microSD, clés USB.

NTFS — New Technology File System. FS de Windows depuis NT.

Over-provisioning — Espace NAND réservé par le contrôleur SSD, invisible utilisateur.

PCB — Printed Circuit Board. Circuit imprimé extérieur d'un HDD ou SSD.

PC-3000 — Plateforme matérielle ACE Lab, standard de facto pour la récupération professionnelle.

PLC — Penta-Level Cell. Mémoire NAND à 5 bits par cellule, 32 niveaux de tension. Annoncée 2023-2025, commercialisation progressive.

PMR — Perpendicular Magnetic Recording. Mode HDD généralisé depuis 2005.

RAID — Redundant Array of Independent Disks. Combinaison de plusieurs disques pour performance ou résilience.

Ransomware — Logiciel malveillant qui chiffre les fichiers et exige une rançon.

Read-retry — Technique de lecture NAND consistant à décaler les seuils de tension pour récupérer une page que la lecture initiale n'a pas pu décoder.

Reverse FTL — Reconstruction logicielle de la table de mapping LBA-NAND d'un SSD à contrôleur défaillant, à partir des métadonnées des pages NAND.

Salle blanche / Cleanroom — Local à atmosphère contrôlée défini par ISO 14644-1. Pour la récupération HDD : ISO Class 5.

Secure Enclave — Coprocesseur de sécurité Apple (iPhone 5s+, Mac T2, Apple Silicon) qui gère les clés cryptographiques.

SED — Self-Encrypting Drive. SSD qui chiffre automatiquement via son contrôleur, standard TCG Opal.

Service Area (SA) — Zone réservée sur les plateaux d'un HDD, invisible à l'OS, contenant plus d'une centaine de modules firmware (P-list, G-list, translator, adaptives).

SMR — Shingled Magnetic Recording. Mode HDD avec pistes partiellement recouvrantes.

Snapshot — Image instantanée d'un volume à coût quasi nul sur les FS copy-on-write.

Spider Web — Procédure d'extraction NAND sur supports monolith (microSD, clés USB tout-en-un). Abrasion laser de la résine puis micro-soudure de 15 à 30 fils de cuivre fins. Documentée publiquement par DAFOTEC.

TCG Opal — Standard du Trusted Computing Group pour le chiffrement matériel des SSD.

TEE — Trusted Execution Environment. Coprocesseur sécurisé Android (équivalent Secure Enclave).

Translator — Module firmware HDD qui convertit LBA en coordonnées physiques (cylindre, tête, secteur). Module 028 sur WD ROYL.

TRIM — Commande ATA (DATA SET MANAGEMENT) ou NVMe (DEALLOCATE) qui informe le contrôleur SSD des LBA libérés côté OS.

UFS — Universal Flash Storage. Successeur d'eMMC pour les smartphones haut de gamme.

VeriFiles — Service Dafotec : le client consulte la liste complète des fichiers récupérables avant tout paiement.

Wear leveling — Stratégie SSD qui répartit les écritures sur toutes les cellules NAND.

WORM — Write Once Read Many. Stockage immuable.

Write blocker — Dispositif matériel ou logiciel bloquant toute écriture vers un support, pour intégrité forensique.

ZFS — Système de fichiers Sun Microsystems (2006), désormais OpenZFS. Copy-on-write, checksums, self-healing.

ANNEXES

Chapitre C

Bibliographie

Sources publiques effectivement consultées pour ce manuel (mai 2026). URLs simplifiées (préfixe https:// et www. omis).

Rapports d'industrie

Verizon Business	2025 Data Breach Investigations Report. Avril 2025.	verizon.com/about/news/2025-data-breach-investigations-report
Backblaze	Drive Stats for 2025. Février 2026.	backblaze.com/blog/backblaze-drive-stats-for-2025/
IBM Security	Cost of a Data Breach Report 2024.	ibm.com/reports/data-breach
ANOZR WAY	Fuites de données 2025. Janvier 2026.	anozrway.com/fr/blog/fuites-de-donnees-en-2025/

Normes

ISO	ISO 14644-1:2015 — Cleanrooms classification.	iso.org/standard/53394.html
ISO	ISO/IEC 27037:2012 — Digital evidence guidelines.	iso.org/standard/44381.html
Trusted Computing Group	TCG Storage Opal 2.0.	trustedcomputinggroup.org/resource/storage-work-group-storage-security-subsystem-class-opal/

Salle blanche et récupération HDD

DriveSavers	Certified ISO Class 5 Cleanroom.	drivesaversdatarecovery.com/why-us/certified-iso-class-5-cleanroom/
Rossmann Group	CMR vs SMR: How Recording Technology Affects Recovery.	rossmanngroup.com/technical-reference/cmr-vs-smr-hard-drives
HackMag	Unmasking Shingled Magnetic Recording in WD and Seagate.	hackmag.com/security/hdd-smr
ACE Lab	PC-3000 documentation publique HDD/SSD modules.	acelab.eu.com/
ISA Group	HDD Service Area Modules Reference.	isa-group.eu/

SSD, NAND, TRIM, FTL

Rossmann Group	What TRIM Does and Why It Destroys Data.	rossmanngroup.com/technical-reference/what-trim-does-and-why-it-destroys-data
Seagate	What Are SSD TRIM and Garbage Collection?	seagate.com/blog/what-are-ssd-trim-and-garbage-collection/
Kingston	The Importance of Garbage Collection and TRIM.	kingston.com/en/blog/pc-performance/ssd-garbage-collection-trim-explained

Lexar Enterprise	Comparing NAND Flash: SLC, MLC, TLC, QLC. 2026.	lexarenterprise.com/comparing-nand-flash-slc-mlc-tlc-qlc-industrial-application/
Belkasoft / Forensic Focus	Recovering Evidence from SSD Drives.	forensicfocus.com/articles/recovering-evidence-from-ssd-drives-in-2014/
DiskGenius	SSD Data Recovery Explained. 2025.	diskgenius.com/resource/ssd-data-recovery-explained.html

Systèmes de fichiers

Sygnia	Forensic Value of MFT Slack Space. 2025.	sygnia.co/blog/the-forensic-value-of-mft-slack-space/
Mahmoud Shaker	MFT, NTFS, $LogFile, $UsnJrnl Forensics. 2025.	mahmoud-shaker.gitbook.io/dfir-notes/
Brian Carrier	File System Forensic Analysis (référence).	sciencedirect.com/topics/computer-science/master-file-table
Number Analytics	Unlocking Ext4: A Forensic Guide. 2025.	numberanalytics.com/blog/ultimate-guide-ext4-digital-forensics

Outils

GNU	GNU ddrescue manual.	gnu.org/software/ddrescue/
CGSecurity	TestDisk and PhotoRec.	cgsecurity.org/wiki/TestDisk
Sleuth Kit	TSK and Autopsy.	sleuthkit.org/
Eric Zimmerman	Forensic tools.	ericzimmerman.github.io/

Sauvegarde

Veeam	3-2-1 Backup Rule Explained.	veeam.com/blog/321-backup-rule.html
Object First	3-2-1-1-0 Backup Rule.	objectfirst.com/blog/how-object-first-and-veeam-bring-3-2-1-1-0-to-life/

Études de cas historiques

Control Engineering	NotPetya / Maersk Throwback Attack. 2025.	controleng.com/throwback-attack-how-notpetya-accidentally-took-down-global-shipping-giant-maersk/
CSO Online	Rebuilding after NotPetya: How Maersk moved forward.	csoonline.com/article/567845/rebuilding-after-notpetya-how-maersk-moved-forward.html
Wired	The Untold Story of NotPetya. 2018.	wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
Threatpost	Code Spaces Out of Business. Juin 2014.	threatpost.com/hacker-puts-hosting-service-code-spaces-out-of-business/106761/
InfoWorld	Murder in the Amazon cloud. 2014.	infoworld.com/article/2179073/murder-in-the-amazon-cloud.html
breaches.cloud / Wiz	Codespaces (2014).	breaches.cloud/incidents/codespaces/

Source DAFOTEC

DAFOTEC	Site officiel : grille tarifaire, expertise technique, études de cas réels, clients institutionnels.	`dafotec.fr`
DAFOTEC Belgique	Version Belgique du laboratoire.	`dafotec.be`

ANNEXES

Chapitre D

À propos de DAFOTEC

DAFOTEC est un laboratoire français de récupération de données fondé à Roubaix en 2004. Le présent manuel a été rédigé par Mhessan Kouassi, expert chez DAFOTEC depuis la création du laboratoire, et bénéficie de 22 années de pratique de terrain et de plus de 120 000 cas traités.

Identité

- **Laboratoire** : 59 Bis rue du Curoir, CS 40082, 59052 Roubaix Cedex (France).
- **Téléphone** : 09 83 70 00 00 (numéro non surtaxé).
- **Sites** : dafotec.fr (France) et dafotec.be (Belgique).
- **Ancienneté** : 22 ans (2004 — 2026).
- **Volume traité** : plus de 120 000 cas depuis 2004.
- **Couverture** : 36 centres de dépôt en France métropolitaine, service d'enlèvement national, laboratoire d'analyse unique à Roubaix.

Certifications et conformité

- **Salle blanche ISO 5** (norme ISO 14644-1) à Roubaix.
- Conformité **RGPD** pour le traitement des données personnelles.
- Conformité **ISO 27001** pour la sécurité de l'information.
- Traitement des supports sensibles sur réseau physiquement isolé d'Internet (**air gapped**).

Clients institutionnels

DAFOTEC est régulièrement retenu par des organismes publics et des institutions scientifiques français pour le traitement de leurs supports en panne, dans le cadre d'accords de confidentialité (NDA). Les donneurs d'ordre cités le sont avec leur autorisation :

- Gendarmerie Nationale
- Centre Hospitalier de Tourcoing
- CNRS (Centre national de la recherche scientifique)
- INSERM (Institut national de la santé et de la recherche médicale)
- Universités françaises

Modèle commercial

- **Diagnostic gratuit** sous 24 heures en laboratoire.
- **Paiement au résultat** : le forfait de récupération n'est facturé qu'en cas de succès. En cas d'échec, seuls 25 € de reconditionnement et de retour sont dus.

- **Service VeriFiles** : la liste complète des fichiers récupérables est communiquée au client *avant tout paiement*. Le client valide cette liste puis décide d'accepter ou de refuser le devis sans frais.
- **Grille tarifaire publique** : 300 € HT pour un disque dur, 400 € HT pour un SSD, 300 € HT pour un smartphone, 550 € HT par disque pour un NAS, 700 € HT par disque pour un RAID. Jusqu'à 950 € HT pour les pannes les plus complexes.

Évaluations indépendantes

4,9/5 sur 797 avis vérifiés Ekomi à la date de publication de ce manuel (mai 2026).

Pourquoi ce manuel est gratuit

Ce livre est distribué gratuitement sous licence Creative Commons BY-NC-ND 4.0, téléchargeable sans inscription depuis dafotec.fr et dafotec.be.

La raison est cohérente avec la mission éditoriale du manuel : réduire la désinformation dans le secteur de la récupération de données ; éviter à des particuliers, à des PME et à des administrations les mauvaises premières décisions qui rendent la récupération impossible ; donner aux techniciens et étudiants en forensique une base francophone solide et sourcée.

DAFOTEC est un laboratoire commercial, mais l'effort de vulgarisation et de transparence technique a une valeur en soi. Si ce manuel évite une mauvaise manipulation, sa rédaction est justifiée. S'il oriente quelques lecteurs vers les bons réflexes (sauvegarde testée, diagnostic avant outil, laboratoire en cas de doute), c'est encore mieux.

Licence de distribution

Creative Commons Attribution — Pas d'Utilisation Commerciale — Pas de Modification 4.0 International (CC BY-NC-ND 4.0).

Vous êtes autorisé à :

- **Partager** — copier, distribuer et communiquer le manuel par tous moyens et sous tous formats.

Selon les conditions suivantes :

- **Attribution** — vous devez créditer DAFOTEC, intégrer un lien vers la licence, et indiquer si des modifications ont été effectuées.
- **Pas d'utilisation commerciale** — vous n'êtes pas autorisé à faire un usage commercial de ce manuel.
- **Pas de modification** — dans le cas où vous remixez, transformez, ou créez à partir du matériel composant ce manuel, vous n'êtes pas autorisé à distribuer la version modifiée.

Fin du manuel. Mai 2026.
DAFOTEC — Roubaix — depuis 2004.

ANNEXES

Chapitre E

Index thématique

Index alphabétique des principaux termes techniques abordés dans le manuel, avec leurs pages d'occurrence. Pour les définitions précises, voir aussi l'annexe B (Glossaire).

A

B

C

D

E

F

G

H

I

J

L

M

N

P

R

S

T

U

V

W

Z

