

ÉDITION 2026

Dafotec France

LABORATOIRE DE RÉCUPÉRATION DE DONNÉES

📖 DOCUMENTATION TECHNIQUE DE RÉFÉRENCE

Guide complet de la récupération de données

Méthodologies, outils, taux de succès et limitations vérifiables sur 6 supports : HDD, SSD, smartphone, RAID, NAS, clé USB et carte mémoire.

Auteur

Mhessan Kouassi
Président de
Dafotec

Dernière mise à jour

26 mai 2026
R&D Dafotec

Public cible

DSI, forensique, CSIRT,
photographes pros,
particuliers

Contact

09 83 70 00 00
contact@dafotec.fr

Plan du guide

Ce guide regroupe la doctrine technique appliquée par notre laboratoire depuis 2004. Chaque chapitre couvre un support de stockage spécifique, décrit la méthodologie d'intervention, nomme les outils utilisés, et fournit les taux de succès vérifiables observés sur les 120 000+ cas traités. Il s'adresse en priorité aux DSI, équipes d'intervention (CSIRT), experts en investigation numérique et photographes professionnels, mais reste accessible à tout particulier exigeant souhaitant comprendre la réalité de la récupération de données.

CHAPITRE 1 Disques durs HDD

Mécanique de précision, salle blanche ISO 5, greffe de têtes

CHAPITRE 2 SSD & NVMe

Reverse FTL, lecture NAND, contrôleurs propriétaires

CHAPITRE 3 Smartphones iPhone & Android

CPU swap, désoxydation, JTAG, déchiffrement Secure Enclave

CHAPITRE 4 Serveurs RAID & NAS

De-striping XOR, reconstruction virtuelle, virtualisation VMware

CHAPITRE 5 Clés USB

Spider Web, Monolith, micro-soudure, rétro-ingénierie FTL

CHAPITRE 6 Cartes mémoire SD, microSD, CF, XQD

Photos RAW, vidéos 4K, drone DJI, GoPro, contrôleurs sécurisés

ANNEXE Glossaire technique

21 termes — FTL, HSA, FAT, BGA, AES, SHR, et autres

Disques durs HDD

Mécanique de précision, salle blanche ISO 5, greffe de têtes

Le disque dur HDD est l'héritage historique du stockage informatique. Bien qu'il soit progressivement remplacé par le SSD sur les postes clients, il reste massivement utilisé sur les serveurs de stockage de masse, les NAS, les enregistreurs vidéo, les sauvegardes externes et tous les usages où la capacité prime sur la vitesse. Sa récupération exige une approche fondamentalement mécanique et électromécanique, qui distingue un véritable laboratoire d'un simple récupérateur logique.

Architecture et points de défaillance

Un HDD comprend des **plateaux magnétiques** tournant à 5 400, 7 200, 10 000 ou 15 000 tours/minute, un **bloc de têtes (HSA — Head Stack Assembly)** survolant les plateaux à 3 nanomètres de hauteur, un **moteur** à coussinet hydrodynamique (FDB), une **carte électronique (PCB)** avec son contrôleur dédié, et une **zone système (Service Area)** sur les plateaux contenant le firmware. Les points de défaillance se répartissent en quatre grandes catégories : mécaniques (têtes, moteur, plateaux), électroniques (PCB, TVS, MOSFET), firmware (Translator, modules, S.M.A.R.T.), et logiques (formatage, suppression, corruption FS).

Phase 1 — Diagnostic et stabilisation

Le diagnostic commence par une inspection au **stéréomicroscope Leica A60** (grossissement 7,5x à 60x) et un test électronique au **SourceMeter Keithley 2450** et **caméra thermique FLIR E5-XT** pour localiser les composants en surchauffe sous courant limité. Identification des défaillances communes : TVS (diodes de protection) détruites après surtension, MOSFET fissurés après dégât liquide, condensateurs gonflés. Pour les disques mécaniques : écoute du pattern sonore (clics simples espacés = problème de têtes, clic continu = problème moteur, sifflement = roulement HS). Documentation photographique des connecteurs et étiquetage selon position physique d'origine. **Aucune écriture sur le disque source** : chaîne de possession forensique.

Phase 2 — Imagerie forensique

Imagerie matérielle simultanée via **DeepSpar Disk Imager** ou **Atola Insight Forensic** avec bloqueurs d'écriture systématiques. Format de sortie : dd brut ou **E01 (EnCase)** forensiquement valide. Génération de sommes de contrôle **MD5 et SHA-256** pour chaque image afin d'assurer l'intégrité. Sur disques instables, gestion stratégique des tentatives de lecture et des délais d'expiration pour empêcher le disque d'entrer dans un état d'erreur fatale. Toute manipulation ultérieure se fait sur l'image clonée, jamais sur le disque source.

Phase 3 — Intervention mécanique en salle blanche ISO 5

Pour les pannes mécaniques : **greffe HSA** (transplantation du bloc de têtes complet) avec stock de disques donneurs catalogués par modèle et révision firmware. Jumelage exact obligatoire : même semaine de production, même masque de lithographie. Alignement micrométrique inférieur à 0,3 µm sous binoculaire à grossissement x60. Pour les cas extrêmes (head crash sévère) : **platter swap** (transfert de plateaux) vers un boîtier mécanique de disque donneur — l'opération la plus délicate du métier, où le moindre désalignement détruit définitivement les données. Reprogrammation des modules adaptatifs propres au disque patient après greffe.

Phase 4 — Reconstruction firmware et accès Service Area

Accès à la zone système via **terminal série spécialisé** branché en mode usine. Patch des modules défectueux : G-List (liste des secteurs réalloués), P-List (liste des défauts d'usine), S.M.A.R.T., zone système. Reconstruction du **Translator** qui convertit les adresses logiques LBA en adresses physiques CHS. Pour les disques **SMR (Shingled Magnetic Recording)** généralisés depuis 2013, utilisation des modules SMR de PC-3000 pour reconstituer simultanément le Translator principal et le cache Translator. Sur disques à hélium (≥ 8 To, scellés), protocole d'ouverture dédié sans risque de fuite.

Probabilités de succès vérifiables

Sur la base de 120 000+ cas traités par Dafotec depuis 2004 : **panne logique standard 95 %**, **panne électronique avec PCB swap + transfert ROM 88 %**, **panne firmware avec accès Service Area 85 %**, **panne mécanique avec disque donneur disponible 78 %**, **plateaux rayés 60 % à 90 %** selon profondeur de la rayure, **head crash sévère 40 %**, **disque tombé dans l'eau (intervention sous 48h) 80 %**, **disque carbonisé par incendie** : diagnostic obligatoire avant engagement.

→ Page service dédiée : dafotec.fr/recuperation-donnees-disques-durs-hdd/

SSD & NVMe

Reverse FTL, lecture NAND, contrôleurs propriétaires

La récupération sur SSD présente un ensemble unique de défis fondamentalement plus complexes que ceux rencontrés sur les HDD ou même les smartphones. L'obstacle principal réside dans l'architecture du SSD, conçue pour la performance et la longévité — pas pour la récupération. La FTL (Flash Translation Layer), le nivellement d'usure agressif, le chiffrement matériel et les contrôleurs propriétaires forment un mur technique que seuls quelques laboratoires dans le monde savent franchir.

Architecture SSD et défis fondamentaux

Un SSD comprend un **contrôleur principal** (Phison, Silicon Motion, Marvell, Samsung, SandForce), un **cache DRAM volatile** (sur les modèles haut de gamme), plusieurs **puces NAND flash** (1 à 16+) et une mémoire **SPI Flash externe** contenant le firmware. Les défis majeurs : la **FTL (Flash Translation Layer)** mappe dynamiquement les LBA vers les pages physiques NAND, stockée dans la DRAM volatile — perdue lors d'une coupure ; le **nivellement d'usure avancé** déplace constamment les données ; le **garbage collection** efface les blocs supprimés en arrière-plan ; le **chiffrement matériel** (TCG Opal, AES-256) lie la clé au contrôleur — sa mort signifie souvent la perte de la clé.

Phase 1 — Diagnostic électronique et réparation niveau composant

Diagnostic au **stéréomicroscope Leica A60**, **SourceMeter Keithley 2450** pour courbes I/V précises, **caméra thermique FLIR E5-XT** pour localisation des composants en surchauffe sous courant limité ($\leq 1V$). Test des composants passifs (résistances, condensateurs, fusibles), actifs (diodes TVS), et identification des symptômes de corruption firmware (disque détecté mais initialisation échoue, capacité incorrecte rapportée, nom générique SATAFIRM S11). Réparation niveau composant : transfert de la **puce SPI Flash** du PCB patient vers PCB donneur identique (modules firmware critiques), remplacement DRAM cache si séparé.

Phase 2 — Mode Service et imagerie native

Entrée en **Mode Service** via **AceLab PC-3000 SSD** et **Stabilisateur DeepSpar SSD**, avec utilitaires propriétaires pour familles de contrôleurs spécifiques (Silicon Motion, Phison, SandForce). Soudage de fils de liaison temporaires sur points de test du PCB pour interrompre le processus de démarrage normal. Édition de modules firmware : **régénération du Traducteur** (force le contrôleur à reconstruire la carte FTL en scannant la NAND), **désactivation de la collecte des déchets** (prévient l'effacement de fond pendant la récupération), correction de modules corrompus, désactivation des sommes de contrôle pour permettre l'initialisation en lecture seule.

Phase 3 — Extraction NAND chip-off (dernier recours)

Méthode la plus complexe et coûteuse, employée quand le contrôleur est physiquement mort. Conduite en **salle blanche ISO 5** sur **station Pace SX-100 ThermoStream** avec préchauffeur. Dessoudage individuel de chaque boîtier NAND (1 à 16+ par SSD). Lecture sur **AceLab PC-3000 SSD** avec attachement lecteur NAND, ou **programmeur RT809H** avec adaptateurs personnalisés. Configuration pour le type NAND spécifique : taille de page, taille de bloc, taille OOB, schéma ECC. Combinaison des vidages NAND en une seule image binaire.

Reconstruction FTL et barrière du chiffrement

Reconstruction : **rétro-ingénierie FTL** (processus mathématique propriétaire pouvant prendre semaines ou mois), analyse de motifs connus (structures FS, chaînes communes), correction ECC (BCH ou LDPC selon génération NAND), assemblage d'image logique exploitable par OS. **Barrière du chiffrement** : si le SSD utilisait un chiffrement matériel (TCG Opal, AES-256) et que le contrôleur est mort, la clé est **définitivement perdue**. Les vidages NAND reconstruits restent du texte chiffré : **récupération techniquement impossible** par quelque méthode que ce soit.

Cas particulier — MacBook à SSD soudé (T2, Apple Silicon M1 à M4)

Sur MacBook fabriqués depuis 2018 (puces T2, Apple Silicon M1, M2, M3, M4), le SSD est **soudé à la carte mère** et chiffré matériellement par le Secure Enclave. Diagnostic aux schématiques Apple et boardview ZXW pour identifier les rails morts (PPBUS_G3H, PP3V3_S5, PP1V8_NAND). Réparation au niveau composant des MOSFET et PMIC grillés, lecture du SSD interne via interface DFU matérielle propriétaire en préservant la chaîne de confiance Secure Enclave. Si la clé FileVault est connue, restitution en clair ; sinon, contenu chiffré uniquement. **Taux de succès** : contrôleur réparable 75-85 %, extraction NAND avec contrôleur connu 50-70 %, contrôleur mort + chiffrement actif 0 %.

→ Page service dédiée : dafotec.fr/recuperation-donnees-disques-durs-ssd/

Smartphones iPhone & Android

CPU swap, désoxydation, JTAG, déchiffrement Secure Enclave

Le smartphone est devenu le support de stockage le plus personnel et le plus exposé : photos d'enfants, contacts professionnels, conversations WhatsApp, données bancaires, identifiants. Sa récupération exige des techniques radicalement différentes du HDD ou du SSD — chiffrement matériel par Enclave Sécurisée, NAND mariée au processeur, soudures BGA microscopiques. L'obstacle principal : accéder à la mémoire NAND brute alors que la carte logique défaillante a brisé la chaîne de confiance cryptographique entre le SOC et la NAND.

Phase 1 — Diagnostic avancé et analyse de défaillance

Inspection au **Stéréomicroscope Leica A60** (7,5x-60x) et **Microscope Trinoculaire AmScope SM-4TZ-144A** (jusqu'à 180x). Examen systématique : corrosion (cartographie de contamination ionique due aux dégâts liquides), stress mécanique (délaminage PCB, billes BGA fissurées), défaillance de composants (PMIC brûlés, condensateurs éclatés). Analyse électronique au **SourceMeter Keithley 2450**, oscilloscope **Rigol DS1202Z-E**, caméra thermique **FLIR E5-XT** : séquençage de l'alimentation (VDD_main, VDD_BOOST), localisation des courts-circuits sous injection $\leq 1V$, vérification des signaux d'horloge critiques (RTC 32,768 kHz, I²C entre PMIC et processeur d'application).

Phase 2 — Scénario A : Réparation et réanimation de la carte

Objectif : atteindre une fonctionnalité minimale pour permettre au SOC et à la NAND de communiquer, autorisant un outil d'extraction logiciel standard (Cellebrite, mode récupération iTunes) à fonctionner. Retravail au niveau composant via **station Pace SX-100 ThermoStream** et préchauffeur **Martin SS-255RF** : rebillage BGA précis, remplacement de CI défectueux (PMIC, EEPROM, contrôleur NAND). Réparation des traces PCB cassées au fil de cuivre émaillé sub-millimétrique sous fort grossissement, masque de soudure polymérisable UV. Conduite en **salle blanche ISO Classe 5**.

Phase 2 — Scénario B : Retrait physique NAND (Chip-Off)

Contournement complet de la carte logique endommagée. Sécurisation sur préchauffeur à 150°C (prévention choc thermique), dessoudage du boîtier NAND avec buse **ThermoStream à 280-320°C** selon taille du boîtier, retrait aux micro-pincettes. Nettoyage de la soudure résiduelle au fer à pointe fine et tresse de cuivre. **Reformage des billes** sur pochoir gravé laser et pâte à souder sans plomb (SAC305). Lecture sur **AceLab PC-3000 Flash**, DeepSpar Disk Imager, ou programmeur universel **RT809H** avec adaptateurs BGA personnalisés (BGA153, BGA162, BGA316).

Phase 3 — Reconstruction logicielle et l'impératif du déchiffrement

L'image NAND brute contient : nivellement d'usure (données dispersées par la FTL), ECC à appliquer, et **chiffrement matériel** (clé UID fusionnée dans le SOC) sur iOS et Android modernes. Analyse de couche de traduction pour rétro-ingénierie de l'algorithme FTL, découpage de système de fichiers (**APFS** pour iOS, **EXT4/F2FS** pour Android), reconstruction de l'arbre de répertoires. **Déchiffrement via technique JTAG / Chip-on** : la carte logique originale doit être réparée juste assez pour alimenter le SOC, pont entre la carte (SOC fonctionnel) et le boîtier NAND monté sur le lecteur, permettant au SOC d'effectuer la négociation cryptographique en temps réel pendant la lecture. Procédure non standard et hautement complexe.

Cas particulier — iPhone et Apple Silicon (A11 à A18 Pro)

Sur iPhone 8 à 17 Pro Max (processeurs Apple A11 à A18 Pro), le **Secure Enclave** protège matériellement les clés cryptographiques. Communication via le protocole **DFU matériel propriétaire d'Apple**, outils dédiés mis à jour à chaque génération iOS. Sur iPhone bloqué erreur 4013/4014, diagnostic DFU pour identifier baseband, Secure Enclave ou NAND. **iPhone reset à distance via Find My iPhone** : le Secure Enclave a détruit la clé ; données définitivement perdues. **iPhone reconditionné** : effacement DFU complet ; données précédentes inaccessibles (garantie du marché reconditionné).

Taux de succès et limitations

Facteurs affectant le succès : dommage NAND physique (fissures = irrécupérable), chiffrement (SOC détruit = déchiffrement impossible), dommage induit par tentatives de réparation précédentes (réduit significativement les chances), expertise du laboratoire. **Probabilité** : réparation board-level réussie 75-92 %, chip-off avec déchiffrement réussi 60-75 %, multiple incident (immersion + écrasement) 40-55 %. **Public cible** : équipes d'intervention sur incident (CSIRT), analystes SOC, ingénieurs en informatique légale, particuliers exigeants.

→ Page service dédiée : dafotec.fr/recuperation-donnees-smartphone/

Serveurs RAID & NAS

De-striping XOR, reconstruction virtuelle, virtualisation VMware

La récupération RAID et NAS constitue **le défi ultime** de la reconstruction de données : tous les défis de la récupération de disque unique combinés au réassemblage de couches logiques avancées.

L'obstacle principal n'est pas la réparation physique d'un disque mais la **reconstruction mathématique du volume virtuel** à partir de plusieurs membres, chacun ayant potentiellement des défaillances individuelles et des métadonnées de configuration obsolètes ou corrompues.

Défis principaux

Scénarios de défaillances multiples : combinaison de défaillances physiques sur un ou plusieurs disques avec corruption logique sur d'autres. **Ambiguïté de configuration** : paramètres RAID manquants ou incorrects (ordre des disques, taille de bande, rotation, direction de parité). **Couches propriétaires** : formats spécifiques (Synology SHR, WD XFS, QNAP LVM) au-dessus des niveaux RAID standard. **Reconstructions à grande échelle** : matrices multi-téraoctets nécessitant des ressources computationnelles spécialisées (stations 64+ cœurs, matrice de stockage 200 To+).

Phase 1 — Triage et documentation forensique

Chaque disque membre est traité comme un cas de récupération individuel. **Imagerie matérielle simultanée** via DeepSpar et Atola sur installation 8+ ports pour prévenir toute dégradation supplémentaire. Étiquetage selon position physique d'origine dans le compartiment, documentation photographique des connecteurs. Acquisition d'**images binaires forensiquement valides** au niveau secteur (format dd ou E01), bloqueurs d'écriture matériels sur tous les disques pendant l'imagerie, génération MD5/SHA-256 pour intégrité. Maintien de la chaîne de possession pour conformité forensique.

Phase 2 — Analyse des paramètres RAID et reconstruction

Extraction automatique des métadonnées via **UFS Explorer, R-Studio, ReclaiMe** : scan des images pour superblocs RAID (linux_raid, lvm2, zfs, etc.). **Analyse manuelle de motifs** à travers les disques pour identifier : taille de bande (64KB, 128KB, 256KB, 512KB, 1MB), direction de rotation (gauche-symétrique, droite-symétrique, asymétrique), calcul de parité (XOR pour RAID 5, XOR double pour RAID 6, Reed-Solomon), ordre original des disques. **Test par force brute** quand paramètres inconnus : exploration systématique de milliers de combinaisons possibles, vérification de parité par cohérence mathématique.

Phase 3 — Émulation de contrôleur virtuel

Création d'un **contrôleur RAID virtuel** reconstituant l'architecture d'origine, présentant la matrice comme un seul volume logique. Outils : **RAID Reconstructor de Runtime, PC-3000 RAID d'AceLab**, scripts personnalisés développés en interne. Reconstruction séquentielle des couches multiples superposées : Hardware RAID → LVM → EXT4/XFS/BTRFS pour les serveurs standards, SHR → MD RAID → LVM → BTRFS pour Synology. **Décodage propriétaire** : **Synology SHR** (allocation dynamique personnalisée), **QNAP LVM-Thick** (gestion volumétrique propriétaire), **Drobo BeyondRAID** (système fermé, options limitées).

Cas particuliers — RAID avancés et virtualisation

RAID 6 : parité double, récupération possible avec deux disques défaillants simultanés. **RAID 10** : miroirs segmentés, récupération avec perte d'un disque par ensemble miroir. **RAID 50/60** : reconstruction des matrices de niveau inférieur puis réassemblage. Une fois le RAID reconstruit, extraction des **machines virtuelles** : scan VMFS pour fragments VMDK (VMware vSphere/ESXi), reconstruction des chaînes de snapshots, remontage virtuel des disques. Compatible Hyper-V (VHDX) et Proxmox (QCOW2). Récupération des bases SQL : MDF/LDF (SQL Server), IBD (MySQL), DBF (Oracle), PG (PostgreSQL).

Taux de succès vérifiables et limitations

Données issues de notre laboratoire (octobre 2025) : **RAID 5 avec 1 disque défaillant : 95-98 %**, **RAID 5 avec 2+ disques défaillants : 60-75 %**, **RAID 6 avec 2 disques défaillants : 90-95 %**, **systèmes propriétaires (SHR, BeyondRAID) : 70-85 %**. **Irrécupérable** : trop de disques défaillants par rapport au niveau de redondance, rebuild ayant écrasé les métadonnées critiques, chiffrement intégral sans clés (LUKS, BitLocker, FileVault sans passphrase). **Ce qu'il ne faut JAMAIS faire** : tenter une reconstruction (rebuild) sur le matériel original, réinitialiser la configuration RAID, formater les disques, utiliser un logiciel grand public sur un array RAID, échanger l'ordre des disques pour tester.

→ Page service dédiée : dafotec.fr/recuperation-de-donnees-serveur-nas-raid-5/

Clés USB

Spider Web, Monolith, micro-soudure, rétro-ingénierie FTL

La récupération sur clé USB représente une catégorie unique au sein du stockage basé sur flash. Elle combine les défis de la mémoire NAND avec une **miniaturisation extrême**, des composants optimisés en coût, et des architectures de contrôleurs diverses. Des milliers de modèles de contrôleurs différents (Phison, Silicon Motion, Alcor, SMI) avec protocoles et micrologiciels propriétaires rendent la communication directe impossible sans outils spécialisés.

Architecture et points de défaillance

Une clé USB moderne comprend un **connecteur USB** (A 2.0/3.0/3.1/3.2, ou C, ou Lightning), un **contrôleur** (cristal oscillateur 12 MHz, régulateurs 3,3V/1,8V), une ou plusieurs **puces NAND**, et parfois des composants de protection (fusibles, TVS). Les clés modernes adoptent une conception **Monolith** : NAND + contrôleur fusionnés dans une résine époxy unique, sans démontage possible. Défaillances communes : connecteur arraché, contrôleur grillé (surtension), NAND dégradée (Bit Rot après stockage prolongé sans alimentation), corrosion (dégât liquide), choc mécanique.

Phase 1 — Diagnostic électronique et analyse d'interface USB

Caractérisation électrique via **analyseur de protocole USB Beagle / Ellisys**, oscilloscope 100 MHz+, alimentation de précision. Mesure de la consommation sur rail 5V pour détecter courts-circuits ou circuits ouverts. **Sondage des lignes D+/D-** pour niveaux de signalisation USB appropriés et diagramme de l'œil. Décodage de protocole : capture de la séquence d'énumération pour identifier les défaillances de communication, tentatives de commandes SCSI standard (INQUIRY, READ CAPACITY), commandes spécifiques fournisseur, accès bas niveau aux registres du contrôleur via utilitaires personnalisés.

Phase 2 — Réparation au niveau composant

Réparation avec **stéréomicroscope Leica A60** et **station de soudage Pace ADS200**, micro-sondes. Procédures courantes : remplacement de l'**oscillateur cristal 12 MHz** défaillant, vérification et remplacement des **régulateurs 3,3V/1,8V**, test et remplacement des composants passifs (résistances, condensateurs, fusibles), refonte ou remplacement des contacts du **connecteur USB**. Sur clés cassées, connecteur arraché, ou pistes brûlées : reconstruction par micro-soudure de fils 0,1 mm entre les broches du contrôleur et les broches USB.

Phase 3 — Extraction NAND et technique Spider Web sur Monolith

Sur clés démontables : dessoudage NAND en salle blanche ISO 5 avec préchauffeur (100°C) et station à air chaud (300-350°C), buse appropriée à la taille du boîtier (TSOP, BGA, LGA). Cartographie de brochage par micro-sondage et référence croisée fiches techniques. Sur clés **Monolith** (tout-en-un en résine époxy) : technique **Spider Web** — **abrasion laser à 1064 nm** de la résine pour exposer les pistes NAND, identification au microscope binoculaire à grossissement x60, puis **micro-soudure de 15 à 30 fils de cuivre de 0,02 mm** sur les broches data NAND. Lecture sur **AceLab PC-3000 Flash**, Flash Extractor, cartes d'adaptation personnalisées.

Reconstruction FTL et système de fichiers

Rétro-ingénierie FTL : analyse de page (4K à 16K), structure de zone de réserve OOB, cartographie des blocs (motifs de nivellement d'usure et d'allocation), application **ECC** appropriée (**BCH** ou **LDPC** selon génération NAND). Reconstruction de l'image logique continue depuis les pages physiques dispersées. **Reconstruction du système de fichiers FAT32/NTFS/exFAT** par sculpture de signatures (en-têtes/pieds de page) et reconstruction de métadonnées. Gestion de la fragmentation par algorithmes avancés. Outils logiciels : UFS Explorer, R-Studio, algorithmes de récupération personnalisés.

Probabilités de succès vérifiables

Corruption logique et défauts électroniques mineurs : > 80 % (formatage, virus, suppression). **Défaillance contrôleur avec extraction NAND** : 50-70 %. **NAND physiquement endommagée ou corrosion sévère** : < 30 %. **Monolith Spider Web** : 75 %. **Impossible** : clés chiffrées sans clés de récupération (BitLocker To Go sans mot de passe, VeraCrypt sans passphrase), NAND avec dommage catastrophique (fracture mécanique du boîtier silicium).

→ Page service dédiée : dafotec.fr/recuperation-donnees-cles-usb/

Cartes mémoire SD, microSD, CF, XQD

Photos RAW, vidéos 4K, drone DJI, GoPro, contrôleurs sécurisés

Les cartes mémoire SD, microSD, CompactFlash, XQD et CFexpress sont les supports de stockage les plus exposés : chocs (chute du drone), humidité (plongée), formatages accidentels en plein shooting professionnel, contacts oxydés. Les photos et vidéos qu'elles contiennent sont souvent **uniques et irremplaçables** : mariage, reportage, voyage. Contrairement aux SSD, les cartes mémoire n'offrent aucune interface standardisée pour l'accès bas niveau, nécessitant matériel spécialisé et rétro-ingénierie.

Architecture et défis spécifiques

Une carte mémoire moderne intègre un **contrôleur sécurisé** (chiffrement des données, restriction de l'accès direct à la NAND), une ou plusieurs **puces NAND** (souvent 3D TLC ou QLC sur les cartes haut de gamme), et une **interface propriétaire** (SD, microSD, CFexpress PCIe, XQD). Défis principaux : **verrouillage du contrôleur**, **gestion flash avancée** (FTL propriétaire, nivellement d'usure, gestion de blocs défectueux, garbage collection), **miniaturisation physique** (puces BGA, pas de 0,4 mm), **diversité NAND** (large variété de types, brochages, configurations à travers fabricants et lignes de produits).

Phase 1 — Test électrique et interrogation contrôleur

Diagnostic via **analyseur de protocole SD/TF Total Phase / Ellisys**, oscilloscope, multimètre de précision. Vérification des courts-circuits sur rails **3,3V et 1,8V**, mesure de consommation pendant l'initialisation. Sondage des lignes **CLK, CMD, DAT0-DAT3** pour niveaux de signal et temporisation appropriés. Décodage de la séquence d'initialisation et des réponses de commande. Interrogation du contrôleur : commandes ATS (Application Specific), lecture **SCR/CSD** (Card Specific Data, Configuration Register), séquences propriétaires connues pour familles de contrôleurs (Phison, Silicon Motion, SK Hynix).

Phase 2 — Réparation PCB ou extraction NAND chip-off

Réparation au niveau PCB avec **stéréomicroscope Leica A60** (7,5x à 60x) et **station Pace ADS200** : nettoyage de précision des contacts dorés avec solvants spécialisés et stylo en fibre de verre, micro-soudure de composants passifs (résistances, condensateurs) au fil 0,3 mm et flux, réparation microscopique de pistes au fil émaillé 0,05 mm et masque de soudure polymérisable UV. En dernier recours en **salle blanche ISO 5** : décapsulation de l'encapsulation époxy via micro-pincettes chauffées et solvants chimiques, dessoudage NAND à 300-350°C avec buse 0,8 mm, cartographie du brochage par micro-sondage.

Phase 3 — Interface NAND directe et rétro-ingénierie

Lecture sur **AceLab PC-3000 Flash** et **Flash Extractor**, cartes d'adaptation personnalisées. Sélection de l'**adaptateur BGA** approprié (BGA100, BGA132, BGA153, BGA162) selon le type de boîtier, séquençage d'alimentation précis (1,8V/3,3V) avec limitation de courant pour prévenir les dommages, configuration de temporisation (tWH, tRH, tADL) selon fiche technique NAND. Rétro-ingénierie FTL : analyse de structure de page (4K à 16K), zone de réserve, schéma ECC. Application correction d'erreur **BCH ou LDPC**, extraction des métadonnées du contrôleur dans les zones de réserve.

Reconstruction par sculpture (data carving) et signatures RAW

Reconstruction du système de fichiers par **sculpture** : recherche des signatures de fichiers dans les données reconstruites. Signatures supportées : JPEG, PNG, MP4, MOV (drone DJI, GoPro 4K), **RAW propriétaires** — CR2 et CR3 (Canon), NEF (Nikon), ARW (Sony), DNG (Adobe/Leica), ORF (Olympus), RAF (Fujifilm), PEF (Pentax), RW2 (Panasonic). Reconstruction même sur cartes formatées ou sans système de fichiers exploitable. Pour les **vidéos 4K fragmentées** : analyse de l'atome moov (index) et chunks mdat, reconstruction des chaînes pour les vidéos en multi-fichiers (limite FAT32 4 Go).

Cas particuliers et taux de succès vérifiables

Cartes CFexpress et XQD : cartes basées PCIe nécessitant des interfaces matérielles spécialisées. **UHS-II et UHS-III** : cartes haute vitesse avec lignes de données supplémentaires et défis de signalisation. **Cartes industrielles** : NAND SLC avec micrologiciel personnalisé et plage de température étendue. **Probabilité de succès** : **corruption logique et défaillances électroniques simples** : > **85 %**, **défaillance contrôleur avec extraction NAND** : **40-60 %**, **boîtiers NAND physiquement endommagés** : < **20 %**. **Impossible** : cartes chiffrées sans clés (rare, sur cartes industrielles haut de gamme), NAND sévèrement endommagées physiquement.

→ Page service dédiée : dafotec.fr/recuperation-donnees-cartes-memoire/

Glossaire technique

Définitions des 21 termes techniques utilisés dans ce guide. Source : documentation R&D Dafotec, normes industrielles, fiches techniques constructeurs.

AES-256

Norme de chiffrement par blocs avec clé de 256 bits, largement utilisée en chiffrement matériel sur SSD, smartphones et cartes mémoire haut de gamme.

Air gapped

Infrastructure réseau physiquement isolée d'Internet, utilisée pour le traitement de supports infectés par ransomware ou contenant des données ultra-sensibles.

BCH / LDPC

Codes de correction d'erreur (Error-Correcting Codes). BCH (Bose-Chaudhuri-Hocquenghem) pour NAND SLC/MLC, LDPC (Low-Density Parity-Check) pour TLC/QLC modernes.

BGA

Ball Grid Array : boîtier de composant avec billes de soudure sous le composant, utilisé pour les puces complexes (CPU, NAND, contrôleurs). Tailles courantes : BGA100, BGA132, BGA153, BGA162, BGA316.

Btrfs

B-tree File System, système de fichiers à arbres B+, snapshots intégrés, utilisé par défaut sur Synology DSM 6+ et certains QNAP.

Chip-off

Technique d'extraction directe d'une puce NAND par dessoudage et lecture sur programmeur externe, utilisée quand le contrôleur est inaccessible.

Chip-on / JTAG

Technique de pont entre une carte logique partiellement réparée et une puce NAND, permettant au SOC d'effectuer la négociation cryptographique en temps réel.

DDF

Disk Data Format, format de métadonnées RAID standardisé par SNIA, utilisé par les contrôleurs Adaptec et LSI MegaRAID.

DFU

Device Firmware Update, mode de communication propriétaire d'Apple utilisé pour la restauration et la récupération bas niveau des iPhone et iPad.

FTL

Flash Translation Layer : couche logicielle dans tout dispositif NAND (SSD, USB, carte SD) qui mappe les adresses logiques LBA vers les pages physiques de la NAND.

HSA

Head Stack Assembly : bloc de têtes complet d'un disque dur HDD, monté sur un actuator. Sa greffe (transplantation) en salle blanche est l'intervention mécanique la plus courante.

LBA

Logical Block Addressing : système d'adressage des secteurs d'un support de stockage par numéro linéaire, traduit en adresses physiques par le firmware.

Monolith

Conception de clé USB ou carte microSD où la NAND, le contrôleur et les composants sont fusionnés dans une résine époxy unique, sans démontage possible.

PCB

Printed Circuit Board, circuit imprimé. Sur un HDD, contient le contrôleur, la mémoire cache, et la ROM avec les paramètres adaptatifs uniques.

SHR

Synology Hybrid RAID, couche au-dessus du RAID Linux mdadm permettant l'utilisation de disques de tailles hétérogènes.

SMR

Shingled Magnetic Recording, technologie HDD où les pistes magnétiques se recouvrent partiellement comme des tuiles. Généralisée depuis 2013 sur les grandes capacités.

Spider Web

Technique propriétaire de récupération sur supports Monolith : abrasion laser de la résine époxy + micro-soudure de 15 à 30 fils de cuivre de 0,02 mm sur les broches NAND exposées.

Translator

Module firmware d'un HDD qui convertit les adresses logiques LBA en adresses physiques (cylindre, tête, secteur). Sa corruption rend le disque détecté mais inaccessible.

TRIM

Commande ATA permettant à l'OS d'informer le SSD des blocs libérés, pour effacement physique en arrière-plan. Effacement irréversible des données supprimées.

VMFS

Virtual Machine File System, système de fichiers propriétaire VMware vSphere/ESXi, contenant les fichiers VMDK des machines virtuelles.

ZFS

Zettabyte File System, système de fichiers avec intégrité par checksum, snapshots, et RAIDZ. Utilisé sur QNAP haut de gamme et TrueNAS.

Besoin d'une intervention experte ?

Dafotec intervient sur tous les supports décrits dans ce guide depuis 2004. **Diagnostic gratuit sous 24h, paiement uniquement en cas de succès**, laboratoire salle blanche ISO 5 à Roubaix, 36 centres de prise en charge en France.

Ligne technique laboratoire

09 83 70 00 00

Du lundi au vendredi, 9h-13h et 14h-18h

Astreinte 24h/7j pour serveurs critiques sous contrat

Laboratoire Dafotec France

59 Bis rue du Curoir, CS 40082

59052 Roubaix Cedex

contact@dafotec.fr

Salle blanche ISO 5 — Accès laboratoire fermé au public, dépôt dans nos 36 centres de prise en charge en France

Engagements Dafotec

- Diagnostic gratuit sous 24h après réception
- Devis ferme avec liste VeriFiles des fichiers récupérables
- Paiement uniquement en cas de récupération réussie (forfait au résultat)
- 25 € de reconditionnement et de retour en cas d'échec ou de refus du devis
- Confidentialité ISO 27001, RGPD, NDA disponible
- 22 ans d'expérience, 120 000+ dossiers traités, 4,9/5 sur 797 avis Ekomi