Dataherstel

Een Referentiehandboek — Editie mei 2026

Door Mhessan Kouassi
Senior Data Recovery Expert bij DAFOTEC

Laboratorium DAFOTEC • Frans laboratorium, ISO 5 cleanroom • Sinds 2004

Anatomie van opslagmedia, professionele methoden, open source en commerciele tools, preventie. Alle kwantitatieve beweringen zijn gesourced of expliciet aangemerkt als grootteorden. Geen verzonnen cases: de aangehaalde historische incidenten zijn openbaar en gerefereerd; de DAFOTEC-labrapporten zijn echte geanonimiseerde cases gepubliceerd op dafotec.fr.

Een naslagwerk voor technici, forensische studenten, gevorderde particulieren en IT-beslissers.

Voorwoord

Waarom dit handboek bestaat — en waartegen het reageert

Ik werk sinds 2004 in dataherstel. In het DAFOTEC-laboratorium in Roubaix (Frankrijk) heb ik meer dan 120.000 opslagmedia geopend, gediagnosticeerd en geimaged — falende harde schijven, stille SSDs, RAID-arrays gedegradeerd door spanningspieken, verbrijzelde smartphones, NAS-units versleuteld door ransomware. Deze praktijk, opgebouwd over 22 jaar, heeft me een simpel ding geleerd: **in dataherstel is de eerste verkeerde beslissing bijna altijd duurder dan de storing zelf**.

Dit handboek is niet geschreven om overal herstel te beloven; het is geschreven om de fouten te vermijden die herstel onmogelijk maken. Dat verschil klinkt bescheiden, maar het tekent de contouren van de hele discipline. Wanneer een klant in het lab arriveert met een klikkende schijf en al drie softwaretools heeft draaien "om te kijken", hebben we niet meer hetzelfde probleem op te lossen als bij het begin van het incident. Wanneer een IT-manager een RAID-rebuild herstart op een gedegradeerde array zonder eerst te imagen, kan de kloof tussen wat herstelbaar was en wat nog is, soms in jaren aan archief worden gemeten.

De sector lijdt aan chronische desinformatie. Consumentensoftware belooft "100%" herstel van bestanden op elk medium. YouTube-tutorials raden de vriezer aan voor harde schijven en rijst voor in water gevallen telefoons. Online vergelijkingen kondigen succespercentages aan met decimalen en zonder gepubliceerde methodologie. Dit handboek is expliciet opgebouwd tegen die literatuur in: elk cijfer is gesourced of aangemerkt als grootteorde, elke methode is gedocumenteerd met haar grenzen, elke belofte is gekwalificeerd door wat zij veronderstelt.

De andere reden voor dit handboek is praktischer. Moderne media — SSDs met agressieve TRIM, Macs met Secure Enclave, door ransomware versleutelde NAS-units, SMR-RAIDs — hebben sommige reflexen achterhaald die we erfden uit het gouden tijdperk van magnetische schijven. Op een HDD uit de jaren 2000 had je dagen of zelfs weken om een verwijderd bestand te herstellen. Op een moderne gezonde NVMe SSD wordt het venster soms in seconden gemeten na TRIM. De discipline is veranderd; de reflexen moeten volgen.

Ik vat hier vier principes samen die 22 jaar praktijk samenvatten:

- **Veldervaring toont aan dat een goedbedoelde verkeerde poging meer data vernietigt dan een eenvoudige logische storing.**
- **In dataherstel beslissen de eerste tien minuten vaak over de volgende tien jaar archief van een bedrijf.**
- **Bij DAFOTEC gaat diagnose altijd voor de tool: we starten geen scan om te kijken, we kwalificeren eerst het risico.**
- **De rol van een serieuze professional is geen wonder te beloven, maar eerlijk te zeggen wat nog herstelbaar is, wat niet meer, en wat vooral niet daarna gedaan mag worden.**

mag het niet doorverkopen, noch een gewijzigde versie publiceren. Deze gratis distributie is een bewuste keuze: wij zien dit handboek liever breed circuleren, want elke vermeden verkeerde eerste beslissing — voor een particulier, een MKB, een IT-afdeling van een ziekenhuis — is meer waard dan wat de verkoop van een paar honderd exemplaren zou opbrengen.

Veel leesplezier. En goede back-ups.

Mhessan Kouassi
Senior Data Recovery Expert • DAFOTEC, Roubaix
Mei 2026

Disclaimer en methodologie

Drie regels stuurden het schrijven van dit handboek:

- Elk percentage is gesourced of expliciet aangemerkt als grootteorde wanneer geen openbare statistiek het rechtvaardigt.
- Geen enkele case is verzonnen. De aangehaalde historische incidenten (NotPetya/Maersk 2017, Code Spaces 2014) zijn openbaar en gerefereerd. De "DAFOTEC-labrapporten" zijn echte interventies, geanonimiseerd, gepubliceerd door DAFOTEC op dafotec.fr.
- De proprietaire DAFOTEC-methoden die in de tekst worden genoemd — VeriFiles, SEAD, HSA-transplantatie, Spider Web, Reverse FTL, CPU Swap — zijn gedocumenteerd op de officiele website; dit handboek presenteert ze in hun technische context.

Voor wie dit boek bedoeld is

IT-technici die met dataverliesincidenten moeten omgaan; studenten digitaal forensisch onderzoek die een pedagogisch overzicht zoeken; gevorderde particulieren die willen begrijpen wat er onder de motorkap gebeurt voordat ze handelen of hun apparaat naar een laboratorium sturen; juristen en gerechtelijke deskundigen die een technische blik nodig hebben om de toelaatbaarheid van digitaal bewijs te beoordelen; managers en CIOs die hun preventiehouding willen evalueren.

Voor wie het niet bedoeld is

Iedereen met een actief noodgeval die geen tijd heeft om te lezen. In dat geval is de regel simpel: **koppel het apparaat los, schrijf er niets op, en raadpleeg ofwel hoofdstuk 5 (diagnose) om uw bearings te vinden, ofwel neem rechtstreeks contact op met een laboratorium**. Diagnose is gratis bij DAFOTEC; u kunt dus een professioneel advies krijgen voor enige financiele beslissing.

Opmerking over prijzen

Alle prijzen die in dit boek worden genoemd (DAFOTEC vaste tarieven in euros) weerspiegelen de Franse markt. Prijzen varieren aanzienlijk tussen landen, tussen laboratoria binnen hetzelfde land, en tussen consumenten- en enterprise-segmenten. Gebruik deze cijfers als grootteorden, niet als internationale referenties.

Juridische kennisgeving

Het herstellen van data van media die niet van u zijn, of die data bevatten beschermd door beroepsgeheim of privacywetgeving (AVG/GDPR in Europa), is gereguleerd. De technieken die hier worden beschreven zijn uitsluitend bedoeld voor educatieve en professionele doeleinden. Voor elke serieuze zaak — medisch, juridisch, intellectueel eigendom — blijft de weg via een laboratorium onder een geheimhoudingsovereenkomst (NDA) de enige aanvaardbare. DAFOTEC werkt onder systematische NDA voor professionele media, conform AVG/GDPR en ISO 27001.

Inhoudsopgave

INLEIDING

Hoofdstuk 0

Dataherstel in 2026

Een discipline op het kruispunt van meerdere vakken

Dataherstel is het geheel van technieken waarmee verloren of ontoegankelijke informatie van een opslagmedium kan worden teruggehaald. De discipline omvat vier vaardighedenfamilies: materiaalfysica (magnetisme voor harde schijven, floating-gate of charge-trap elektronica voor NAND-geheugen), bestandssysteem-algoritmen, reverse engineering van proprietaire controllers, en forensische procedurele rigor.

Het wordt zorgvuldig onderscheiden van **backup restore**, dat onder preventie valt. Herstel komt na het verlies, op een apparaat dat geen bruikbare kopie heeft. Het is per definitie een spoeddiscipline waarin men werkt met wat over is.

Twee werelden, nooit te verwarren

Logisch herstel: het apparaat is fysiek intact en wordt door de machine herkend. Het probleem zit in de software — corrupt bestandssysteem, verwijderde partitie, gewiste bestanden, ransomware-versleuteling. De ruwe data is bijna altijd nog aanwezig; men moet alleen weten hoe ze te lezen.

Fysiek herstel: hardwarestoring. Het apparaat wordt niet meer herkend, of geeft abnormale geluiden, of de controller reageert niet meer. De interventie vereist een gespecialiseerde omgeving: cleanroom voor mechanische schijven, micro-soldering station voor SSDs.

Alle hersteltrajecten beginnen met een diagnose die tussen deze twee werelden beslist. De verkeerde wereld kiezen kost data. Hoofdstuk 5 beschrijft deze stap.

De evolutie sinds 1990

Drie decennia lang vond herstel plaats op magnetische harde schijven. Het principe was stabiel: zolang de platters niet fysiek werden overschreven, bleef de data ter plaatse. Verwijdering, snelle formattering, logische corruptie: deze raakten alleen de toewijzingstabel, niet de inhoud. Het was het gouden tijdperk van consumentensoftware zoals Norton Utilities of, later, TestDisk.

De massale komst van SSDs vanaf 2010 verschoof de discipline. NAND-geheugen gedraagt zich niet als een magnetische schijf: er kan niet ter plekke worden overschreven, en de controller moet voortdurend hele blokken consolideren en wissen. Met het **TRIM**-commando (geintroduceerd in Windows 7, macOS 10.6.8 en Linux-kernel 2.6.33) activeert het wissen van een bestand een *fysieke* wissing van de betreffende cellen, vaak binnen seconden tot minuten. Op een moderne gezonde SSD krimpt het logische herstelvenster dramatisch.

Parallel hebben twee andere ontwikkelingen het landschap hervormd: de verspreiding van **hardwarematige versleuteling** (SED, TCG Opal, BitLocker met TPM, FileVault met Secure Enclave) die fysieke data onbruikbaar maakt zonder de sleutel, en de explosie van **ransomware**-aanvallen die nu expliciet op back-ups gericht zijn. Verizon DBIR 2025 kwantificeert deze laatste trend: ransomware was in 2024 betrokken bij 44% van de gedocumenteerde datalekken, een stijging van 37% op jaarbasis.

Over statistieken — Er bestaan geen openbare geconsolideerde statistieken die het globale slaagpercentage van dataherstel geven. Professionele laboratoria publiceren soms cijfers in hun marketingmateriaal. DAFOTEC publiceert die van zichzelf openbaar op dafotec.fr — per storingstype, over de 120.000+ behandelde cases sinds 2004: 95% bij logische HDD-storingen, 88% bij elektronische HDD-storingen, 78% bij mechanische HDD-storingen, 82% bij SSD-firmwarestoringen, 61% bij SSD-NAND-storingen, 91% bij gedegradeerde RAID 5, 69% bij smartphones. Deze cijfers gelden alleen voor DAFOTEC, op een scope van cases die niet zijn verergerd door eerdere pogingen. Zij weerspiegelen historische prestaties, geen garantie op een individueel geval.

Hoe dit boek is georganiseerd

Zeven delen, negentien hoofdstukken, vijf bijlagen. De progressie is doelbewust: eerst begrijpen wat een opslagmedium *fysiek* is (deel I), dan hoe een storing te diagnosticeren (deel II), dan welke methoden toe te passen (deel III), dan bijzondere gevallen aan te pakken (deel IV), dan in de praktijk de juiste tools te kiezen (deel V), dan hoe dit alles overbodig te maken via goede preventie (deel VI), en tot slot waar de discipline de komende jaren heen gaat (deel VII).

Vier lay-outconventies:

- **Blauwe** kaders zijn pedagogische opmerkingen.
- **Oranje** kaders zijn operationele waarschuwingen — te lezen voor men handelt.
- **Groene** kaders zijn openbaar gesourcede casestudy's (publiek gedocumenteerde historische incidenten).
- **Beige** kaders met de aanduiding "LABRAPPORT — DAFOTEC" zijn echte geanonimiseerde interventies, gepubliceerd door DAFOTEC op haar officiele website.

Deel I

Fysieke fundamenten

Voor elke methode moet men *fysiek* begrijpen hoe data wordt geschreven, gelezen en verwijderd. Drie hoofdstukken: een mechanische harde schijf (HDD), een NAND-geheugen (SSD, eMMC, UFS, SD-kaart), en een bestandssysteem (de logische laag die blokken in een boomstructuur organiseert). Zonder deze basis zijn de methoden van de volgende hoofdstukken louter magie.

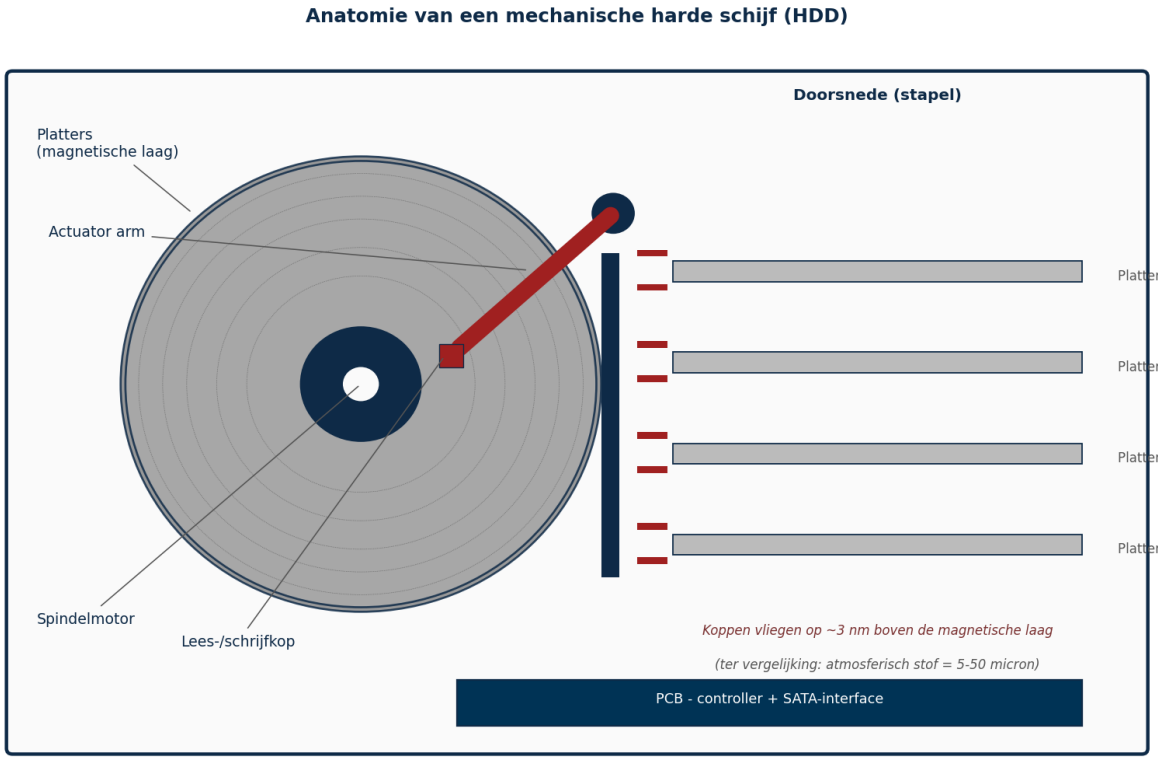
DEEL I — FYSIEKE FUNDAMENTEN

Hoofdstuk 1

Anatomie van een mechanische harde schijf

1.1 Overzicht

Een harde schijf (HDD) is een geminiaturiseerd precisie-mechanisme. Onder de hermetisch gesloten behuizing bevinden zich: een of meerdere rigide **platters** bedekt met een magnetische laag, een **spindelmotor** die ze met constante snelheid laat draaien, **lees-/schrijfkoppen** gedragen door een **actuator arm** die het oppervlak afveegt, en een externe **printplaat** (PCB) met de controller, de firmware-ROM en de SATA- of SAS-interface.



Schematische anatomie van een 3,5"-HDD: platters, arm, koppen in nanometrische vlucht, PCB.

Typische grootteorden voor een 3,5" consumenten-HDD in 2026:

Parameter	Typische waarde
Rotatiesnelheid	5.400 of 7.200 RPM (consument), tot 15.000 (enterprise SAS)
Capaciteit per platter	2 tot 4 TB
Aantal platters	1 tot 10 afhankelijk van totale capaciteit
Lineaire dichtheid	Meer dan 1 miljoen bits per spoorinch
Vlieghoogte koppen	Enkele nanometers boven de platter
Sequentiele doorvoer	150 tot 300 MB/s

Parameter	Typische waarde
Random-access latentie	5 tot 15 ms

1.2 Hoe data wordt geschreven

De magnetische laag van de platter is verdeeld in miljarden kleine magnetische domeinen. De schrijfkop, door een zeer sterk en zeer kort lokaal magnetisch veld op te wekken, orienteert de polarisatie van een domein in de ene richting (bit 1) of de andere (bit 0). De overgang tussen twee tegengestelde polarisaties is wat de leeskop later detecteert, door inductie of recenter door tunnel-magnetoresistief effect (TMR).

Zolang niets de zone overschrijft, zijn deze magnetische polarisaties **stabiel over decennia**. Dat is de fundamentele eigenschap die HDDs zo herstelbaar maakt: het wissen van een bestand op bestandssysteem-niveau raakt de magnetische domeinen zelf niet.

1.3 PMR, CMR, SMR, HAMR: de schrijftechnologieen

Vier technologieen bestaan naast elkaar of volgen elkaar op:

- **PMR** (Perpendicular Magnetic Recording): sinds 2005 worden magnetische domeinen loodrecht op het oppervlak georienteerd in plaats van parallel. Basis van alle moderne HDDs.
- **CMR** (Conventional Magnetic Recording): moderne term voor "klassiek" PMR met niet-overlappende sporen. Maakt het mogelijk elk spoor te overschrijven zonder buren te raken.
- **SMR** (Shingled Magnetic Recording): sinds 2013 overlappen sporen elkaar gedeeltelijk als dakpannen. Winst van 20 tot 25% in dichtheid, maar elke wijziging van een spoor vereist het herschrijven van de hele band naburige sporen.
- **HAMR** (Heat-Assisted Magnetic Recording): technologie die het domein kortstondig verhit per laser tijdens het schrijven. Gecommercialiseerd vanaf 2024 op zeer hoge-capaciteit enterprise-schijven (30 TB+).

SMR en herstel — SMR is duidelijk complexer te herstellen bij firmwarestoring: de vertaling tussen logische adressen (LBA) en fysieke locaties op de band wordt door de controller beheerd, en corrupte firmware kan inhoud onleesbaar maken zelfs op intacte platters. Laboratoria gebruiken gespecialiseerde modules (PC-3000 heeft sinds 2020 SMR-modules gepubliceerd). Bron: Rossmann Group, *CMR vs SMR: How Recording Technology Affects Recovery*, 2026.

1.4 Typische mechanische storingsoorzaken

1. **Head crash.** Een kop komt in contact met het platteroppervlak. Resultaat is vaak een progressieve kras die de magnetische laag fysiek vernietigt. Klassiek symptoom: *herhaalde klikken* van de kop die tevergeefs probeert te positioneren.
2. **Stiction.** Koppen blijven aan de platter plakken in plaats van correct te parkeren. De motor kan de rotatie niet meer starten. Symptoom: *kort gezoem dan stilte*.
3. **Spindelmotor-uitval.** Lagers slijten, motor draait vast. Symptoom: *platter draait helemaal niet meer, of schoksgewijs*.
4. **PCB doorgebrand.** Een spanningspiek vernietigt componenten van de printplaat, vaak de TVS. De schijf wordt helemaal niet meer gedetecteerd; soms rookt hij letterlijk.

5. **Firmwarecorruptie.** De PCB-ROM of een systeemzone van de platters (Service Area) wordt onleesbaar. De schijf draait maar mount niet, of mount met een absurde capaciteit (0 GB, 8 MB, inconsistente waarde).

> **Let op —** Een klikkende HDD moet onmiddellijk worden uitgezet. Elke extra platterrotatie waarbij de koppen het oppervlak raken verlengt de gekraste zone — per seconde gaat data verloren. Dit is een van de zeldzame echte noodgevallen in herstel.

1.5 Waarom een HDD zeer herstelbaar blijft

Wanneer een bestandssysteem een bestand verwijdert, wijzigt het alleen zijn eigen interne tabellen (MFT voor NTFS, inodes voor ext4, FAT-tabel voor FAT32/exFAT). De fysieke sectoren die het bestand bevatten worden noch gewist, noch gedemagnetiseerd. Dat gebeurt pas wanneer een nieuw bestand ze overschrijft.

Daarom is op een HDD:

- Een verwijderd bestand herstelbaar zolang zijn sectoren niet zijn hergebruikt.
- Een snelle formattering reinitialiseert alleen de basisstructuren van het FS.
- Een volledige formattering (die alles herschrijft) vernietigt de data effectief, maar duurt uren en wordt bijna nooit per ongeluk gedaan.

Op een niet-overschreven HDD halen logische hersteltools (TestDisk, R-Studio, UFS Explorer, PhotoRec als laatste redmiddel) in de praktijk de overweldigende meerderheid van de data terug.

1.6 De gemiddelde betrouwbaarheid van een HDD in 2026

Backblaze publiceert sinds 2013 uitvalstatistieken voor zijn HDD-vloot. Het jaarrapport 2025 (gepubliceerd in februari 2026) telde 344.196 schijven verspreid over 30 modellen. Drie kerncijfers:

- Jaarlijkse AFR 2025: **1,36%** (gedaald van 1,55% in 2024).
- Lifetime AFR over de levensduur: **1,30%**, stabiel kwartaal op kwartaal.
- Q4 2025 toonde een kwartaal-AFR van 1,13%, het laagste sinds 2022.

Met andere woorden: op een massale steekproef faalt ongeveer 1,4% van de schijven per jaar. Voor een particulier met een enkele schijf zegt dat individueel niet veel. Maar het herinnert eraan dat over een vloot, uitval statistisch zeker is.

Bron: Backblaze, Drive Stats for 2025, jaarrapport gepubliceerd 12 februari 2026.

1.7 Service Area, firmware modules, translator

Een cruciaal deel van de intelligentie van een HDD bevindt zich noch op de PCB, noch in de controller, maar in een specifieke zone van de platters zelf: de **Service Area** (SA), onzichtbaar voor het besturingssysteem. Ze bevat meer dan honderd firmwaremodules. Drie families verdienen genoemd te worden:

- **P-List** (Primary defect list, module 0A op WD ROYL). Lijst van defecte sectoren geidentificeerd *in de fabriek*.
- **G-List** (Grown defect list, module 0B). Sectoren die defect zijn geworden *tijdens de levensduur* en die firmware automatisch heeft hertoegewezen aan reservesectoren.

- **Translator** (module 028 op WD ROYL). Centrale module die de logische adressen (LBA) vertaalt naar fysieke adressen op de platters. Zijn corruptie maakt een mechanisch perfect gezonde schijf *volledig onleesbaar* door het OS.
- **Adaptives** (modules 102 tot 109 op WD). Kopkalibratieparameters, specifiek voor elk schijfexemplaar. Dit is wat een eenvoudige PCB swap onmogelijk maakt.

Op een SMR-schijf is de translator nog kritischer: hij moet ook de mapping tussen CMR-cachezones en shingled bands beheren. Herstel bestaat dan uit het **reconstrueren of repareren van de translator** met gespecialiseerde tools zoals PC-3000 — in de praktijk gebeurt dit dagelijks in uitgeruste laboratoria. Bronnen: ACE Lab, Rossmann Group, ISA Group *HDD Service Area Modules Reference*.

Diagnose van een SA-storing — Typisch symptoom van Service Area-corruptie: de schijf wordt gedetecteerd door de BIOS maar toont een absurde capaciteit (0 GB, 8 MB, plausibele maar verkeerde waarde). De schijf draait normaal, geeft geen abnormale geluiden — het is puur logisch aan de interne firmwarekant. Diagnose voorbehouden voor het laboratorium: de TTL-seriele terminal op de PCB is nodig om toegang te krijgen tot de SA.

LABRAPPORT — DAFOTEC • WD Blue 2 TB harde schijf, koppen defect (case #1)

Apparaat: WD Blue 2 TB 3,5" • **Doorlooptijd:** 72 uur • **Vast tarief:** 650 EUR (Franse markt)

Symptoom. Herhaalde klikken om de 3 seconden, schijf niet gedetecteerd, na een val van 80 cm op tegelvloer van de externe behuizing.

Interventie. Opening in ISO 5 cleanroom, vervanging van de kopstapel (HSA) door een identieke donorschijf met overeenstemmende firmware-revisie, met sub-micron uitlijning onder 0,3 micron. Sector-voor-sector klonen met verkorte timeout om de nieuwe koppen/platters-combinatie te sparen.

Resultaat. 1,94 TB hersteld van 2 TB. 3 gedeeltelijk corrupte 4K-videos konden niet volledig worden teruggehaald vanwege een licht gekraste platterzone veroorzaakt door de val.

Professionele fotograaf, regio Parijs - 4 jaar archief gered. Case gepubliceerd op dafotec.fr.

DEEL I — FYSIEKE FUNDAMENTEN

Hoofdstuk 2

Anatomie van een SSD: NAND, controller, FTL

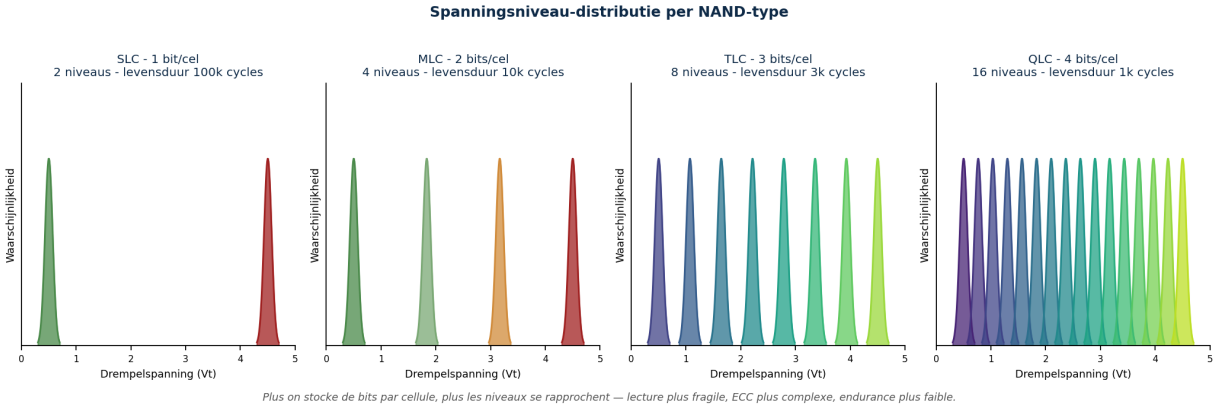
2.1 Een paradigmaverschuiving

Een SSD (Solid State Drive) heeft geen mechanische onderdelen. Alle complexiteit zit in de elektronica. Dat klinkt als een vereenvoudiging, maar voor herstel is het tegendeel waar: NAND-geheugen legt fysieke beperkingen op die de controller dwingen om verwijderde data actief te wissen. Op een HDD vernietigt verwijderen niets; op een moderne SSD *vernietigt* verwijderen binnen de volgende minuten.

2.2 NAND-cellen: floating-gate en charge-trap

De fundamentele eenheid is de NAND-cel. Historisch was het een **floating-gate** transistor. Sinds de 3D-NAND-generaties (2013, daarna massaal vanaf 2017) is de technologie verschoven naar **charge-trap flash** (CTF). In plaats van een geleidende gate wordt een isolator gebruikt die elektronen vangt. Voordelen: betere slijtagebestendigheid, eenvoudiger 3D-fabricage, minder lekkage tussen naburige cellen.

Afhankelijk van het aantal spanningsniveaus dat in een enkele cel wordt onderscheiden, worden meer of minder bits opgeslagen. Dit is de kernafweging tussen dichtheid, levensduur en betrouwbaarheid:



Hoe meer bits per cel, hoe dichter de niveaus.

Type	Bits/cel	Niveaus	Levensduur (P/E)	Gebruik
SLC	1	2	50.000 tot 100.000	Industrieel, kritiek enterprise
MLC	2	4	3.000 tot 10.000	Enterprise (in verval)
TLC	3	8	1.000 tot 3.000	Gangbare consumenten-SSD 2026
QLC	4	16	150 tot 1.000	Hoge capaciteit budget
PLC	5	32	minder dan 150 (schatting)	In ontwikkeling

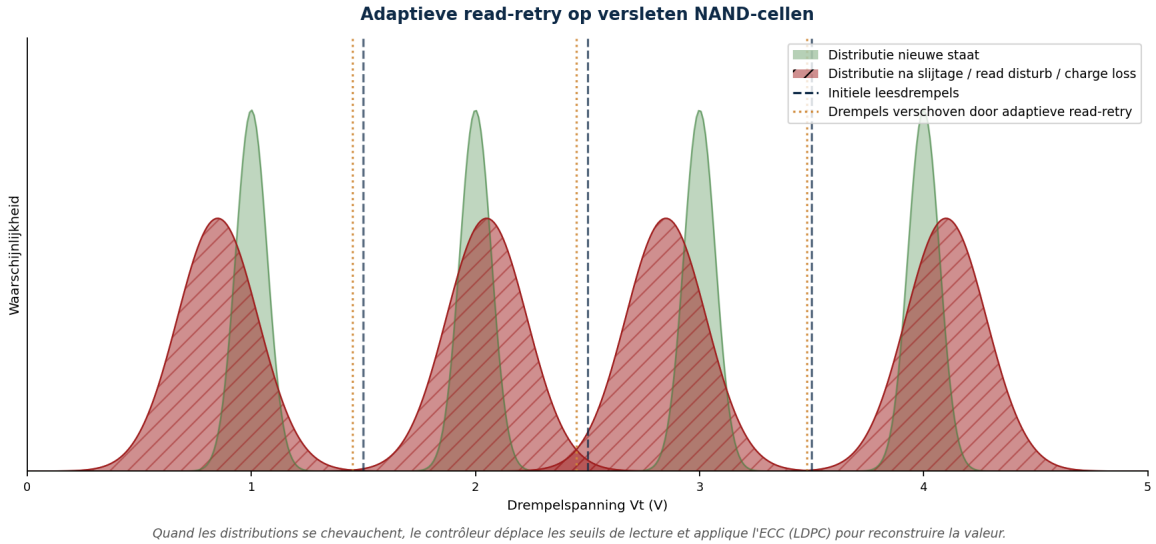
Hoe meer bits per cel worden opgeslagen, hoe smaller de marge tussen niveaus (in QLC minder dan 200 mV tussen twee aangrenzende staten), hoe frequenter de leesfouten, hoe meer de controller

ECC moet toepassen, en hoe sneller de cel slijt.

2.3 ECC, LDPC en adaptieve read-retry

Naarmate marges krimpen, evolueren foutcorrigerende codes. De eerste MLC-SSDs gebruikten **BCH**-codes. Moderne TLC/QLC-SSDs gebruiken bijna allemaal **LDPC**-codes (Low-Density Parity-Check), krachtiger maar complexer.

Wanneer de ruwe lezing te veel fouten produceert, activeert de controller de **read-retry**: hij wijzigt de spanningsreferentie en herleest dezelfde pagina, soms vijf, tien of vijftien keer met verschillende drempels.



Read-retry verschuift drempels om overlappende distributies te onderscheiden.

ECC en chip-off — Voor chip-off herstel vormt dit alles een grote moeilijkheid: ruwe NAND lezen buiten haar originele controller betekent data verkrijgen na scrambling en voor ECC-decoding. Men moet zowel de scrambler als de ECC-pipeline reverse-engineeren.

2.4 De fundamentele beperking: schrijven per pagina, wissen per blok

NAND-geheugen kan worden gelezen en geschreven op **pagina**-niveau (typisch 4, 8 of 16 KB), maar kan alleen worden gewist op **blok**-niveau (256 tot 512 paginas). Ter plekke overschrijven is onmogelijk: het hele blok moet eerst worden gewist.

Om performant te blijven doet de controller dit nooit naief. Wanneer een bestand wordt gewijzigd:

1. Schrijft hij de nieuwe versie naar een vrije pagina, elders op NAND.
2. Werkt hij zijn interne mappingtabel bij (**FTL — Flash Translation Layer**) zodat de logische LBA nu naar de nieuwe pagina wijst.
3. Markeert hij de oude pagina als ongeldig maar wist hij ze niet meteen.
4. Later consolideert de **garbage collector** de resterende geldige paginas en past hij de wisspanning toe op lege blokken.

2.5 Wear leveling, over-provisioning, hardwarematige versleuteling

Aangezien elke cel een beperkte levensduur heeft, past de controller **wear leveling** toe: hij verspreidt schrijfacties over alle beschikbare cellen. Een zone **over-provisioning** (minimaal 7%, vaak 14% tot 28% op enterprise-SSDs) is onzichtbaar voor de gebruiker.

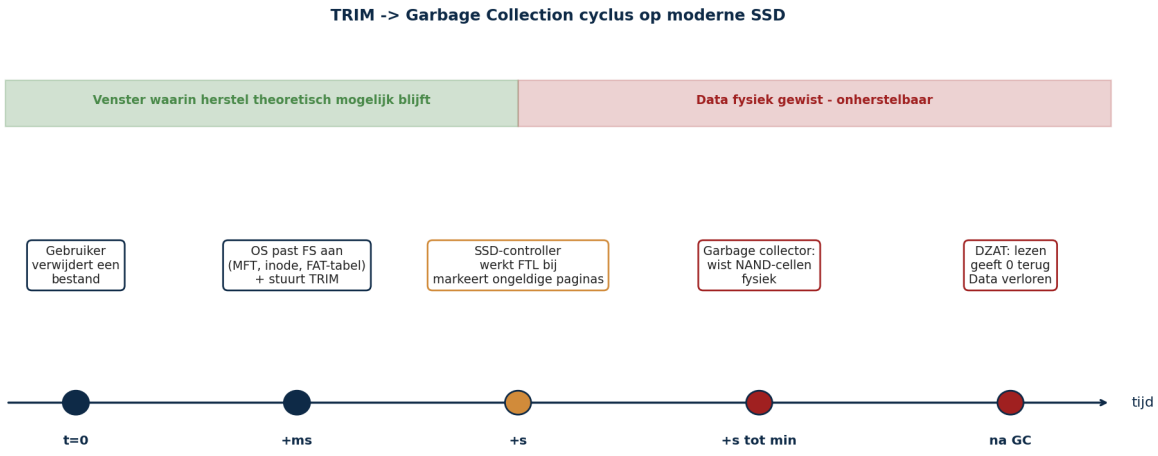
Vaak genegeerd kritisch element: op de meerderheid van moderne SSDs is **alle NAND-inhoud hardwarematig versleuteld met AES-256**, zelfs wanneer de gebruiker geen wachtwoord heeft ingesteld. De masterkey wordt afgeleid van een unieke controller-identifier (UID). Wanneer de controller sterft, gaan zowel de FTL-tabel als de sleutel verloren.

2.6 TRIM: het commando dat alles verandert

Zonder TRIM heeft de controller geen idee welke paginas op bestandssysteem-niveau nog in gebruik zijn. **TRIM** (ATA-commando DATA SET MANAGEMENT of NVMe DEALLOCATE) lost dit op door de controller te informeren over LBAs die OS-zijde zijn vrijgemaakt. De controller kan dan:

- Zijn mappingtabel onmiddellijk bijwerken.
- Deze blokken plannen voor fysieke wissing bij de volgende garbage-collection-cyclus.

Op de meeste moderne SSDs die DRAT of DZAT implementeren, geeft elke daaropvolgende lezing van getrimde LBAs ofwel een deterministische niet-gespecificeerde waarde terug, ofwel nullen. Logische hersteltools zien niets bruikbaars meer.



TRIM dan garbage collection cyclus: het herstelvenster sluit binnen seconden tot minuten.

2.7 Het herstelvenster

Op een moderne NVMe SSD met TRIM actief:

- Bij verwijdering van een bestand: TRIM wordt onmiddellijk verzonden (milliseconden).
- De garbage collector kan binnen seconden tot maximaal minuten activeren.
- Eenmaal het blok fysiek gewist, recupereert geen enkele chip-off nog iets.

> **Let op —** Als u een belangrijk bestand heeft verwijderd van een SSD: **koppel het apparaat onmiddellijk los**, sluit het niet weer aan op dezelfde machine, en stuur het voor analyse. Elke seconde onder spanning vermindert de kansen.

2.8 Wanneer TRIM niet werkt

SSD-herstel blijft mogelijk in verschillende configuraties waar TRIM kortgesloten is:

- **Hardware RAID.** De meeste RAID-controllers geven TRIM niet door.
- **Externe SSDs via oude USB-SATA-bruggen.** Oudere JMicron JMS539 en ASMedia ASM1051 geven TRIM niet door.
- **NAS.** Afhankelijk van firmware en configuratie kan TRIM afwezig of vertraagd zijn.
- **Low-end pseudo-SSDs.** Sommige USB-sticks en SD-kaarten implementeren TRIM niet.
- **Buggy firmware.** Verschillende modellen werden uitgeleverd met defecte TRIM.
- **Kleine bestanden intern opgeslagen in NTFS MFT.** Bestanden onder ~700 bytes worden direct in de MFT-entry opgeslagen en nooit door TRIM geraakt.
- **Fragmenten in nog gedeeltelijk gebruikte blokken.** Zolang een blok minstens een geldige pagina bevat, kan het niet volledig worden gewist.

2.9 Hoe controleren of TRIM actief is

```
Windows: fsutil behavior query DisableDeleteNotify
(0 -> TRIM ingeschakeld, 1 -> uitgeschakeld)

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

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


DEEL I — FYSIEKE FUNDAMENTEN

Hoofdstuk 3

Bestandssystemen: de schatkaart

3.1 Waarom het bestandssysteem beslist

Het bestandssysteem (FS) is de softwarelaag die een ruw blokapparaat omvormt tot een boom van benoemde bestanden. Wanneer een bestand wordt verwijderd, wijzigt het FS doorgaans twee of drie van zijn interne structuren. De inhoud van het bestand zelf wordt niet geraakt. Het is deze asymmetrie die logisch herstel mogelijk maakt.

3.2 FAT32 en exFAT: eenvoud

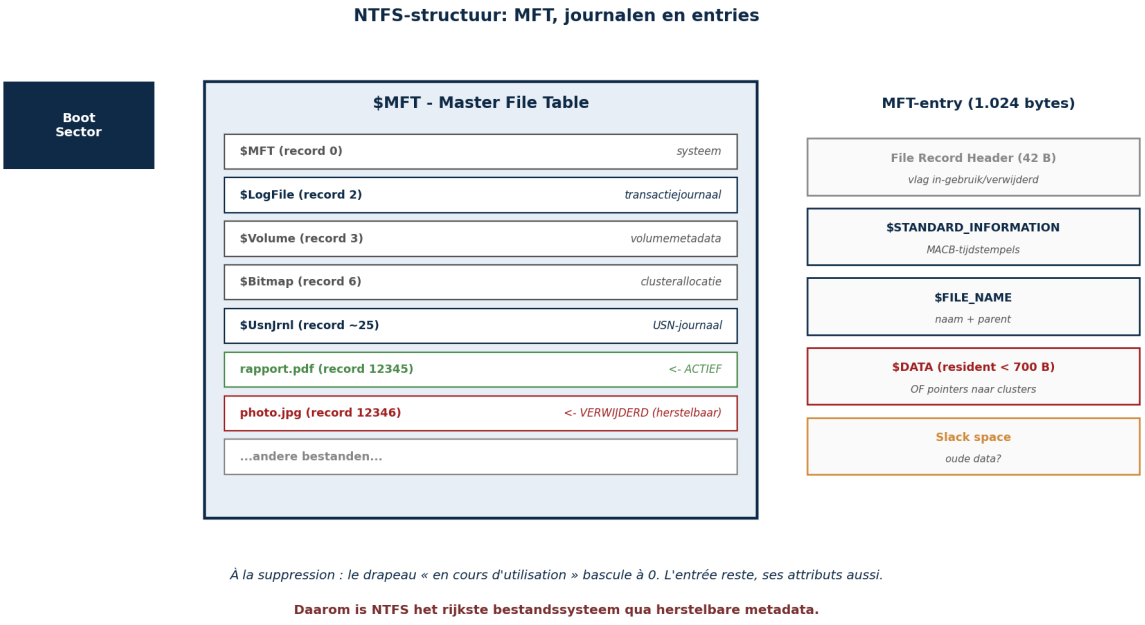
FAT32 is beperkt tot 4 GB per bestand; exFAT (2006) heft deze limiet op en is de cross-platform standaard geworden. Structuur: een bootsector, een of twee FAT-tabellen, en de rest van het volume als datazone. Bij verwijdering:

- Het eerste teken van de directory-entry wordt vervangen door 0xE5.
- De clusters in de FAT-tabel worden als vrij gemarkeerd.
- De inhoud van de clusters blijft intact tot overschreven.

Herstel is over het algemeen zeer effectief op FAT/exFAT, vooral voor aaneensluitende bestanden. Hoofdbeperking: de eerste letter van de naam is verloren.

3.3 NTFS: de forensische rijkdom

NTFS (Microsoft, 1993) is het standaard Windows-FS. Het is technisch het FS met de meeste residuele metadata.



NTFS-structuur: Boot Sector, $MFT en 1.024-byte entries.

De centrale structuur is de **Master File Table** ($MFT): een speciaal bestand met een 1.024-byte entry voor elk bestand. Deze entry omvat:

- Een header (eerste 42 bytes) met een vlag die aangeeft of de entry in gebruik of verwijderd is.
- Een $STANDARD_INFORMATION-attribuut met de vier MACB-tijdstempels.
- Een $FILE_NAME-attribuut met de naam.
- Een $DATA-attribuut met ofwel direct de inhoud (indien < ~700 bytes), ofwel pointers naar dataclusters.

3.4 Multi-source temporele correlatie op NTFS

De ware kracht van NTFS in forensiek komt naar voren wanneer meerdere metadatabronnen worden gecorreleerd:

- De **$MFT** en zijn twee sets tijdstempels ($STANDARD_INFORMATION en $FILE_NAME). Divergentie tussen de twee is een klassieke marker van manipulatie.
- Het $LogFile-transactiejournaal.
- Het $UsnJrnl:$J-USN-journaal.
- De **Windows event logs** (.evtx).
- Het **register** (UserAssist, ShellBags, MUICache).

Typische workflow: exporteer de $MFT naar CSV met MFTECmd (Eric Zimmerman), het $LogFile met LogFileParser, het $UsnJrnl met UsnJrnl2Csv, voeg ze samen in een timeline-tool. Deze multi-source benadering is onmisbaar zodra er een juridische inzet is.

NTFS slack space — Voor herstel van verwijderde bestanden blijft NTFS het meest permissieve FS: de MFT-entry blijft na verwijdering, met al haar attributen. Referentie: Sygnia, *The Forensic Value of MFT Slack Space*, 2025.

3.5 ext4: de Linux-specificiteit

ext4 (2008) is het standaard FS van de meeste Linux-distributies. Drie kernelementen: **superblock**, **inode-tabel**, **extents**.

Bij verwijdering op ext4:

1. De inode wordt vrij gemarkeerd in de inode-bitmap.
2. De extents worden vrijgegeven in de blok-bitmap.
3. In de inode zelf wist ext4 gedeeltelijk de pointers naar blokken (in tegenstelling tot ext3 dat ze bewaarde).

De referentietool is **extundelete** (open source). Wanneer dat faalt, staat **debugfs** toe de structuur handmatig te onderzoeken:

```
$ sudo debugfs /dev/sda1
debugfs: lsdel
debugfs: stat <12345>
debugfs: dump <12345> /pad/bestand.bin
```


Let op — Op ext4, als u zojuist iets belangrijks heeft verwijderd, remount de partitie onmiddellijk read-only: sudo mount -o remount,ro /dev/sdXY. Elke schrijfactie, zelfs een eenvoudige systeemlog, kan vrijgegeven inodes hergebruiken.

3.6 APFS: copy-on-write en snapshots

APFS (Apple, 2017) is gebaseerd op twee principes:

- **Copy-on-write.** Elke wijziging schrijft elders en werkt pointers bij.
- **Snapshots.** APFS kan momentopnames van eerdere volume-staten bewaren tegen marginale kosten.

Gevolg voor herstel: op een onversleutelde APFS kunnen weken geleden verwijderde bestanden aanwezig zijn in een lokale snapshot. Tools zoals R-Studio, UFS Explorer en Disk Drill exploiteren deze snapshots.

De muur is FileVault. Standaard ingeschakeld op moderne Macs met Apple Silicon, versleutelt FileVault het hele volume met AES-256. Zonder het wachtwoord is de fysieke data slechts een pseudo-willekeurige stroom.

3.7 Btrfs en ZFS: maximale robuustheid

Btrfs (2009) en ZFS (2006) zijn copy-on-write FS met checksums en snapshots, ontworpen voor veerkracht op schaal.

- **Checksums.** Elk blok wordt beschermd door een checksum.
- **Self-healing.** Automatische correctie op mirror of RAID-Z.
- **Snapshots.** Kritiek na ransomware: de meeste NAS-ransomware versleutelt zichtbare bestanden maar raakt read-only snapshots niet aan (hoofdstuk 12).

3.8 Samenvattende tabel

FS	Platformen	Gedrag bij verwijdering	Logisch herstel
FAT32	USB, SD	Entry 0xE5, FAT gereset	Zeer goed
exFAT	USB, SD	Zoals FAT32, uitgebreid	Zeer goed
NTFS	Windows	MFT bewaard, $LogFile en $UsnJrnl	Uitstekend
ext4	Linux	Inode vrijgegeven, extents gewist	Middelmatig
APFS	macOS, iOS	Copy-on-write, snapshots	Uitstekend via snapshots
Btrfs / ZFS	NAS, Linux	Copy-on-write, snapshots	Uitstekend via snapshots

Deel II

Diagnose

Voor het handelen, het begrijpen. Twee hoofdstukken: een gekwantificeerd overzicht van de oorzaken van dataverlies in 2025-2026, en een triagemethode.

DEEL II — DIAGNOSE

Hoofdstuk 4

Oorzaken van dataverlies: cijfers 2025-2026

4.1 Vier oorzaakfamilies

- **Menselijk en logisch**: accidentele verwijdering, formattering, configuratiefout.
- **Cyber**: ransomware, destructieve malware, wipers.
- **Hardware**: mechanische storing, elektronische storing, NAND-slijtage.
- **Omgeving**: brand, overstroming, spanningspiek, diefstal.

4.2 Ransomware, de nieuwe norm

Het Verizon DBIR 2025-rapport is de statistische referentie over datalekken.

Indicator	Waarde 2024	Trend
Ransomware in inbreuken	44%	+37% vs DBIR 2024
Ransomware in MKB	88%	Verslechterend
Ransomware in grote ondernemingen	39%	Stabiel
Gestolen credentials	22%	Nog steeds #1
Uitgebuite kwetsbaarheden	20%	+34%
Mediaan losgeld	$115.000	Dalend
Weigerde te betalen	64%	+14 pt in 2 jaar

Bron: Verizon Business, 2025 DBIR, gepubliceerd 23 april 2025.

De pessimistische lezing: ransomware is een dominante modus operandi geworden. De optimistische: het mediane losgeld daalt, twee op drie slachtoffers weigeren nu te betalen.

4.3 Menselijke fout, nog steeds de meerderheid

Het menselijke element blijft betrokken bij 60% van alle bestudeerde inbreuken (DBIR 2025). Voor dataherstel specifiek: accidentele verwijdering van bestanden, foutieve formattering, overschrijving door verkeerde manipulatie, massale verwijdering door script, verlies van wachtwoord.

4.4 Gemiddelde hardwarebetrouwbaarheid

Voor HDD's blijft Backblaze de openbare referentie: jaarlijkse AFR van 1,36% over 337.192 productieschijven eind 2025. Voor SSDs bestaat geen vergelijkbaar grootschalig openbaar rapport.

4.5 Samenvatting

1. **Menselijke fout** blijft de nummer een oorzaak in volume.
2. **Ransomware** is geexplodeerd tot de eerste oorzaak in financiele impact.

3. **Hardwarestoringen** nemen langzaam af op HDDs; op SSDs minder frequent maar vaak catastrofaler.
4. **Omgevingsincidenten**: enkele procenten, maar massieve kosten mogelijk.

DEEL II — DIAGNOSE

Hoofdstuk 5

Diagnose en triage

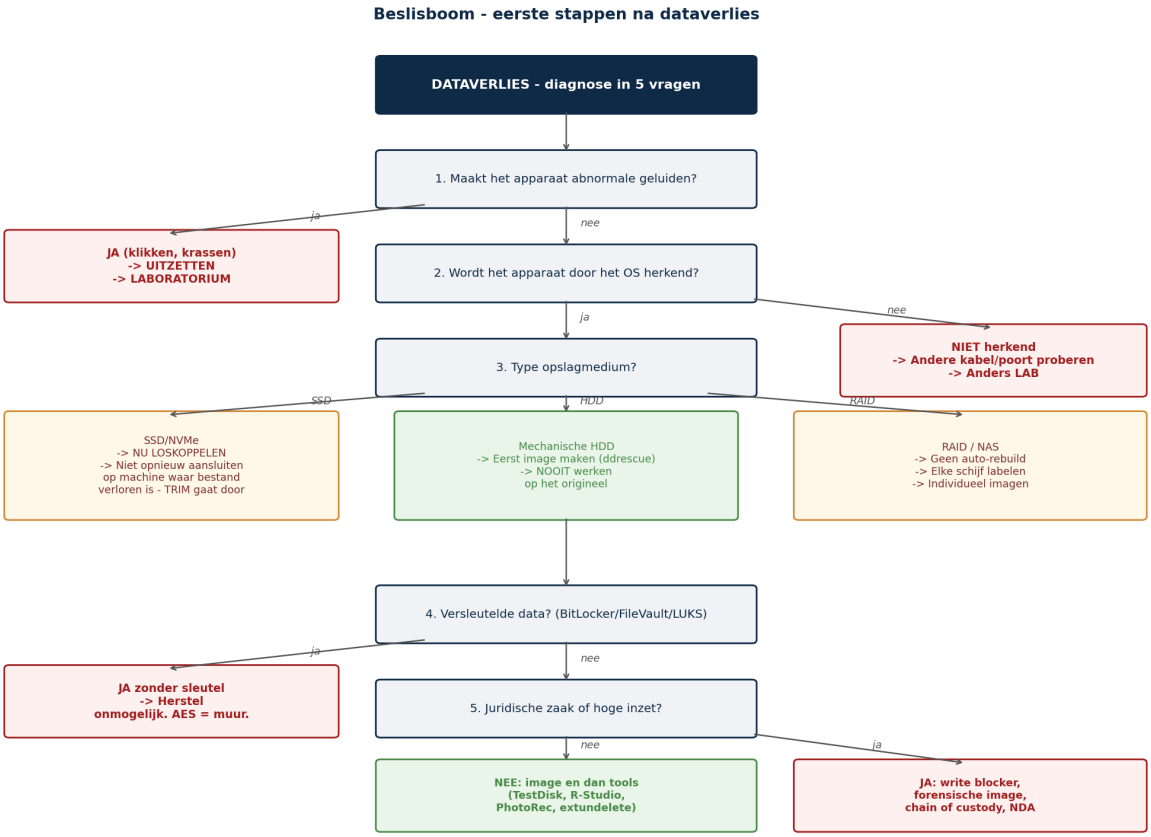
5.1 Waarom diagnose de kritieke stap is

Diagnose beslist over alles: tussen software- of fysieke interventie, persoonlijke poging of laboratorium, voorspelbare kosten, en vaak de uitkomst zelf.

> **Let op —** Zolang de diagnose niet is gesteld, raak niets aan. Vooral, start geen enkele hersteltool om te kijken.

5.2 Triage-procedure in vijf stappen

1. **Observeer.** Heeft het apparaat stroom? Maakt het geluid? Wordt het door BIOS/OS gedetecteerd?
2. **Classificeer.** Als fysiek, logisch of hybride.
3. **Beoordeel de inzet.** Onvervangbaar? Juridisch, medisch, professioneel?
4. **Beslis het pad.** Persoonlijke interventie, technicus, of lab.
5. **Documenteer.** Foto's, serienummers, traceer elke manipulatie.



Snelle beslisboom na dataverlies.

5.3 Typische symptomen en hun betekenis

Symptoom	Waarschijnlijke diagnose	Onmiddellijke actie
Herhaalde klikken op HDD	Defecte koppen - fysiek	Onmiddellijk uitzetten
Stille HDD, niet gedetecteerd	PCB of motor defect	Uitzetten, lab
HDD met absurde capaciteit	Corrupt Service Area	Lab (PC-3000)
SSD helemaal niet gedetecteerd	Controller defect	Uitzetten, lab
SSD met vreemde capaciteit	Corrupte firmware	Lab
Ontbrekende partitie	Logisch	ddrescue, TestDisk
Bestanden gewist op HDD	Logisch - breed venster	Loskoppelen, imagen
Bestanden gewist op SSD	Logisch - kort venster	ONMIDDELLIJK LOSKOPPELEN
RAW-volume	Logisch	Imagen dan R-Studio
Bestanden met onbekende extensies	Ransomware	Hoofdstuk 12
Wachtwoordprompt op hele schijf	BitLocker/FileVault/LUKS	Herstelsleutel vinden

5.4 Wanneer naar een laboratorium gaan

Drie criteria, waarvan er ten minste een volstaat:

- Niet gedetecteerd of abnormale geluiden → lab.
- Onvervangbare en kritieke data → lab, zelfs voor eenvoudige gevallen.
- U heeft al iets geprobeerd dat de situatie verergerde → stop, laat een pro beoordelen.

5.5 Een laboratorium kiezen

Seriositeitscriteria:

- Gecertificeerde ISO 5 cleanroom (ISO 14644-1).
- Gratis diagnose en betaling bij succes.
- Lijst van herstelbare bestanden voor betaling (DAFOTEC noemt deze dienst "VeriFiles").
- Schriftelijke vertrouwelijkheid (NDA).
- Verifieerbare reputatie. Internationale referenties: Ontrack, Kroll, DriveSavers, SalvageData, Gillware. Voor Frankrijk: DAFOTEC in Roubaix (ISO 5 sinds 2004, publieke klanten: Franse Nationale Politie, UMC Tourcoing, CNRS, INSERM, Franse universiteiten).

Tekenen van een dubieus laboratorium — Als u wordt gevraagd om volledige betaling voor diagnose, of een gegarandeerd slaagpercentage wordt beloofd, vertrek dan.

Deel III

Methoden

Zes hoofdstukken die het operationele hart vormen.

Drie gouden regels — Drie transversale regels gelden voor al deze hoofdstukken: (1) **eerst imagen**; (2) **nooit naar het bronapparaat schrijven**; (3) op SSDs met TRIM, **elke seconde onder spanning vermindert het venster**.

DEEL III — METHODEN

Hoofdstuk 6

Veilig imagen

6.1 Het principe

Imagen bestaat uit het maken van een bit-voor-bit kopie van het bronapparaat naar een imagebestand. Het origineel wordt apart gelegd. Drie redenen:

1. **Redden wat te redden valt.** Een falend apparaat faalt vaak meer in de volgende uren.
2. **Rustig werken.** Op de image kunt u zoveel pogingen doen als u wilt.
3. **Bewijs bewaren.** In forensiek wordt het origineel verzegeld; al het werk wordt op een kopie gedaan (ISO 27037).

6.2 ddrescue: de referentietool

GNU ddrescue is de open source referentietool. Zijn superioriteit boven dd berust op drie elementen: een mapfile, een multi-pass leesstrategie, fijne afhandeling van foutsectoren.

Typische workflow

Identificeer het apparaat precies:

```
$ lsblk -o NAME,SIZE,MODEL,SERIAL,TRAN
# Het serienummer bevestigt dat we de juiste schijf targeten.
```

Eerste pass, snel:

```
$ sudo ddrescue -f -n -d /dev/sdX /pad/image.img /pad/image.map
-f : staat output naar een apparaat toe
-n : 'no-scrape': blijft niet hangen op moeilijke zones
-d : directe toegang tot het apparaat
```

Tweede pass, gericht op moeilijke zones met retries:

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

Op een klikkende schijf vermijden we boven -r3: elke poging is een kans extra om het oppervlak te beschadigen.

Eenmaal de image verkregen

```
$ sha256sum /pad/image.img > /pad/image.img.sha256
$ sudo losetup --read-only --find --show /pad/image.img
$ sudo mount -o ro,noload /dev/loop0 /mnt/recovery
```

> **Let op —** Bewaar de mapfile en image op een ander apparaat dan de bron.

6.3 Alternatieven voor ddrescue

FTK Imager (gratis, Windows), **Guymager** (Linux GUI), **dc3dd** (forensiek), **PC-3000 Disk Imager**, **DeepSpar**, **Atola Insight Forensic** (lab hardware).

6.4 Write blockers

Voor forensische zaken: hardware write blocker tussen bron en analysemachine. Referenties: Tableau, WiebeTech. Voor cautious gebruik: blockdev --setro op Linux volstaat.

DEEL III — METHODEN

Hoofdstuk 7

Logische analyse en FS-reparatie

7.1 Het principe

Eenmaal de image verkregen, zoekt logische analyse de FS-structuren te repareren of interpreteren. Bijna altijd effectiever dan carving.

7.2 TestDisk: de partitietabel

TestDisk (CGSecurity) is de referentietool voor het repareren van MBR- en GPT-partitietabellen.

1. Start testdisk /pad/image.img.
2. Selecteer schijf, tabeltype.
3. Run "Quick Search" dan eventueel "Deeper Search".
4. Controleer en schrijf weg ("Write").

7.3 NTFS: MFT, $LogFile, $UsnJrnl

- **R-Studio** en **UFS Explorer** (commercieel) voor NTFS-reconstructie.
- **MFTECmd** (Eric Zimmerman, gratis) parseert $MFT naar CSV.
- **The Sleuth Kit** + **Autopsy**: open source framework.

```
$ fls -r -p image.img > files.txt
# Verwijderde bestanden gemarkeerd met '*'
$ icat image.img 12345 > hersteld.bin
```

7.4 ext4: extundelete, debugfs

```
$ sudo extundelete --restore-file 'home/user/belangrijk.pdf' /dev/sdb1
$ sudo extundelete --restore-all /dev/sdb1

$ sudo debugfs /dev/sdb1
debugfs: lsdel
debugfs: dump <1234> /tmp/hersteld
```

7.5 APFS: snapshots exploiteren

```
$ tmutil listlocalsnapshots /
$ diskutil apfs listSnapshots /Volumes/data
```

7.6 Btrfs en ZFS: snapshots en herstel

```
$ sudo btrfs subvolume list /volume1
$ cp /volume1/.snapshots/123/bestand.pdf /volume1/

$ sudo zfs list -t snapshot
```

Op Synology DSM 7 / QNAP QTS 5 NAS-units zijn Btrfs-snapshots standaard ingeschakeld. Daarom worden ransomware-aanvallen (eCh0raix, QlockerBunny, DeadBolt) vaak omzeild zonder te betalen.

DEEL III — METHODEN

Hoofdstuk 8

Diepgaand data carving

8.1 Wanneer te carven

Data carving reconstrueert bestanden door hun handtekeningen te zoeken in ruwe data, zonder FS-structuren. Laatste-redmiddel-operatie.

8.2 Vier niveaus van verfijning

Niveau 1 — Eenvoudige handtekening

Formaat	Header (hex)	Footer
JPEG (JFIF)	FF D8 FF E0	FF D9
PNG	89 50 4E 47 0D 0A 1A 0A	49 45 4E 44
PDF	25 50 44 46 ("%PDF")	%%EOF
ZIP / DOCX	50 4B 03 04	Variabel
MP4 / MOV	(offset 4) 66 74 79 70	Geen vaste footer
SQLite	53 51 4C 69 74 65 ...	—

Zeer effectief op **niet-gefragmenteerde** bestanden. Tools: **PhotoRec**, **Foremost**, **Scalpel**.

Niveau 2 — Semantisch carven

Exploiteert interne structuren (PDF xref-tabel, ZIP central directory). Maakt gefragmenteerde reconstructie mogelijk.

Niveau 3 — Entropie-analyse

Shannon-entropie per blok onderscheidt tekst / compressie / versleuteling.

Niveau 4 — Machine learning

Recente benaderingen (2023-2026). Belkasoft X en Magnet AXIOM kondigden ML-modules aan. Veelbelovende maar beperkte resultaten.

8.3 PhotoRec: de open source standaard

```
$ sudo photorec /pad/image.img
```

PhotoRec is traag: reken op meerdere uren voor 1 TB.

> **Let op —** PhotoRec herstelt **nooit** originele namen — het hernoemt ze f0000001.jpg, enz.

8.4 Harde grenzen van carving

- **Fragmentatie.** Op gefragmenteerde FS: eerste fragment dan ruis.

- **Versleuteling.** Maximale entropie, lijkt op geen enkel formaat.
- **Compressie.** Een ZIP/MP3/JPEG die zijn eerste blokken kwijt is, is onherstelbaar.
- **Vals-positieve.** Op 1 TB ruwe NAND: miljoenen bestanden, 99% ruis.

DEEL III — METHODEN

Hoofdstuk 9

Fysieke interventie op HDD

9.1 De cleanroom: waarom het niet onderhandelbaar is

De koppen van een HDD vliegen enkele nanometers boven de magnetische laag. Atmosferisch stof (typisch 5 tot 50 micron) gevangen onder een bewegende kop is op schaal het equivalent van een auto met 200 km/u tegen een betonnen muur. De magnetische laag wordt gekrast, vaak onherstelbaar.

Om een harde schijf te openen zonder de platters te vernietigen, is een omgeving vereist waar de deeltjesconcentratie drastisch is verlaagd. ISO 14644-1 classificeert cleanrooms per maximale deeltjesconcentratie:

ISO-klasse	Deeltjes >=0,5 micron / m<super>3</super>	Typisch gebruik
ISO 1	10	Ultra-precieze halfgeleider
ISO 2	100	Spitsonderzoek
ISO 3	1.000	Geavanceerde cleanroom
ISO 4	10.000	Standaard halfgeleider
ISO 5	100.000	Professioneel HDD-herstel
ISO 6	1.000.000	Onvoldoende voor HDDs
Omgevingslucht	~35.000.000	Buiten scope

De standaard voor HDD-herstel is ISO 5. Dat is wat serieuze internationale laboratoria hebben (DriveSavers, SalvageData, Gillware, Secure Data Recovery, Ontrack) en in Frankrijk bij DAFOTEC in Roubaix.

Let op — Een HDD openen in een gewone kamer, zelfs een schone, is vrijwel zekere extra vernietiging. YouTube-videos waarin amateurs een head swap in hun garage doen zijn onverantwoord.

9.2 Head swap (kop-transplantatie)

Wanneer de koppen falen, worden ze vervangen door die van een fysiek identieke **donor**-schijf. Procedure:

1. Diagnose bevestigend dat de platter-mechanica intact is en dat we te maken hebben met een kopprobleem.
2. Sourcing van een strikt identieke donorschijf. Laboratoria houden voorraden van honderden modellen.
3. Opening van beide schijven onder laminaire flow, demontage van kop/arm-assemblages met speciale gereedschappen.
4. Overdracht van de kop/arm-assemblage van donor naar patient.

5. Sluiting van de patient, inschakelen.
6. Onmiddellijke imaging met hardware-imager (PC-3000, DeepSpar).

De donor moet identiek zijn tot op de firmware-revisie. Een ogenschijnlijk identiek donormodel maar van een andere firmware-revisie kan een schijf opleveren die draait maar niets leest.

9.3 PCB swap en ROM-herprogrammering

Als de storing op de externe printplaat zit (spanningspiek, doorgebrande TVS), kan de PCB worden vervangen door die van een donor. Maar pas op: op de meeste moderne schijven zijn kalibratieparameters specifiek voor het fysieke apparaat (bad sector map, kopparameters) opgeslagen in een ROM op de PCB. Zonder overdracht van deze ROM produceert de patient-schijf met donor-PCB in het beste geval onleesbare data.

9.4 Bijzondere gevallen

9.4.1 SMR-schijven

SMR-schijven (zie 1.3) stellen specifieke uitdagingen. Wanneer firmware of de translatiezone corrupt is, moeten de LBA-mappingen worden gereconstrueerd rekening houdend met de cache en de bands. PC-3000 publiceerde sinds 2020 dedicated SMR-modules. Slaagpercentage blijft lager dan equivalente CMRs.

9.4.2 Stiction

Wanneer koppen aan de platter blijven plakken bij start, kan men ze handmatig "loswrikken" in de cleanroom door de platters met de hand te draaien terwijl kort spanning wordt aangelegd. Zeer delicaat — er is risico om de magnetische laag onder de koppen af te scheuren.

9.4.3 Gekraste platters

Als de kras oppervlakkig en gelokaliseerd is, kan wat buiten de gekraste zone ligt vaak worden hersteld (met verloren sectoren). Als de kras diep of uitgebreid is, is het terminaal — de magnetische laag is afgescheurd.

9.5 Professionele hardwareplatforms

- **PC-3000** (ACE Lab, Rusland): globale de facto standaard. Modules voor HDD, SSD, Flash, RAID, mobiel.
- **DeepSpar Disk Imager** (Canada): zeer effectief alternatief voor HDD-imaging.
- **Atola Insight Forensic**: geavanceerde forensiek.

Volledige laboratoriumuitrusting (PC-3000 HDD + Flash + Express + adapters + micro-solderingstools + ISO 5 cleanroom) vertegenwoordigt een investering van enkele tienduizenden euros. Dit is de hoofdreden waarom fysiek herstel in elk serieus laboratorium minstens enkele honderden euros kost.

DEEL III — METHODEN

Hoofdstuk 10

Fysieke interventie op SSD

10.1 Waarom het moeilijker is dan een HDD

Op een HDD is de data magnetisch en persistent. Op een SSD is de data:

- Elektrisch (lading gevangen in cellen), dus potentieel vluchtig.
- Scrambled door de controller — descrambling moet bekend zijn.
- Gecodeerd met een ECC eigen aan de controller.
- Logisch gemapped door een FTL die alleen de originele controller perfect kent.
- Vaak hardwarematig versleuteld (SED, TCG Opal).

Drie interventietechnieken, in volgorde van voorkeur (minst destructief eerst):

10.2 JTAG / ISP: niet-destructief

Moderne SSD-controllers exposeren vaak testpunten corresponderend met een intern debugprotocol: **JTAG** of **ISP**. Door tijdelijk dunne draden op deze punten te solderen, en aan te sluiten op een gespecialiseerde programmer, kan men:

- De controller-firmware lezen.
- Een herstel-*loader* injecteren die de dode firmware omzeilt.
- De controller laten spreken alsof hij normaal werkte.

Voordelen: de NAND wordt gelezen door zijn originele controller, dus descrambling en ECC worden automatisch afgehandeld. Hardwarematige versleuteling blijft ontsleuteld. Het fysieke apparaat wordt niet vernietigd.

Nadelen: vereist gespecialiseerde tools (PC-3000 Flash met JTAG-adapters), goede precisie micro-solderingsvaardigheden, en kennis van testpunten per controller-familie.

10.3 Chip-off: de laatste-redmiddel-techniek

Als JTAG faalt of niet toepasbaar is, worden de NAND-chips fysiek gedesoldeerd om onafhankelijk van de controller te worden gelezen.

10.3.1 Fysieke verwijdering

Moderne NAND-chips zijn in BGA-packaging met tientallen tot honderden soldeerballen onder de component. Desolderen vereist:

- Een gekalibreerd heteluchtsoldeerstation met precies thermisch profiel.
- Thermische bescherming van de rest van de PCB (kapton, hitteschilden).
- Een binoculaire microscoop om de chips op leessockets te herpositioneren.

10.3.2 De lezing

Eenmaal de chip gedesoldeerd en gereinigd, wordt hij op een universele NAND-programmer gelezen: PC-3000 Flash, Soft-Center Flash, FlashExtractor.

10.3.3 Logische reconstructie (de echte uitdaging)

Op dit stadium hebben we een ruwe dump per NAND-chip. Om bruikbare data te extraheren moeten we:

1. **Descrambelen** van de paginas. De originele controller paste een XOR toe met een pseudo-random reeks afhankelijk van het adres. Zonder de LFSR-polynoom te kennen, onmogelijk te inverteren.
2. **ECC decoderen**. Moderne controllers gebruiken LDPC met honderden pariteit bits per pagina. Zonder reproductie van deze pipeline gaat veel data verloren.
3. **Paginas herassembleren**. Op multi-chip SSDs zijn logische paginas verdeeld tussen chips volgens een interleaving-schema. Deze volgorde moet worden gereconstrueerd.
4. **FTL reconstrueren**. Vanuit metadata ingebed in elke pagina (spare area), de LBA → fysieke locatie mappingtabel reconstrueren. Het meest complexe werk.
5. **Als de SSD hardwarematig versleuteld was**, en de controller-sleutel kon niet worden hersteld — het is voorbij.

10.4 Apple Silicon: maximale moeilijkheid

Macs met T2-chip (2018+) of Apple Silicon M1/M2/M3/M4 integreren de SSD-controller in de CPU/SoC zelf:

- De NAND is direct op het moederbord gesoldeerd.
- De SSD-controller zit in de SoC.
- Hardwarematige versleuteling is gebonden aan een unieke ID van de **Secure Enclave**.
- FileVault is standaard ingeschakeld op Apple Silicon.

Voor herstel zonder gebruikerswachtwoord: onmogelijk. Als het wachtwoord bekend is maar het moederbord defect is, kunnen gespecialiseerde laboratoria de kritieke componenten (CPU/SoC met Secure Enclave) transplanteren naar een blanco donor-moederbord. DAFOTEC documenteert deze interventie publiek onder de naam "Mobile CPU Swap" voor smartphones.

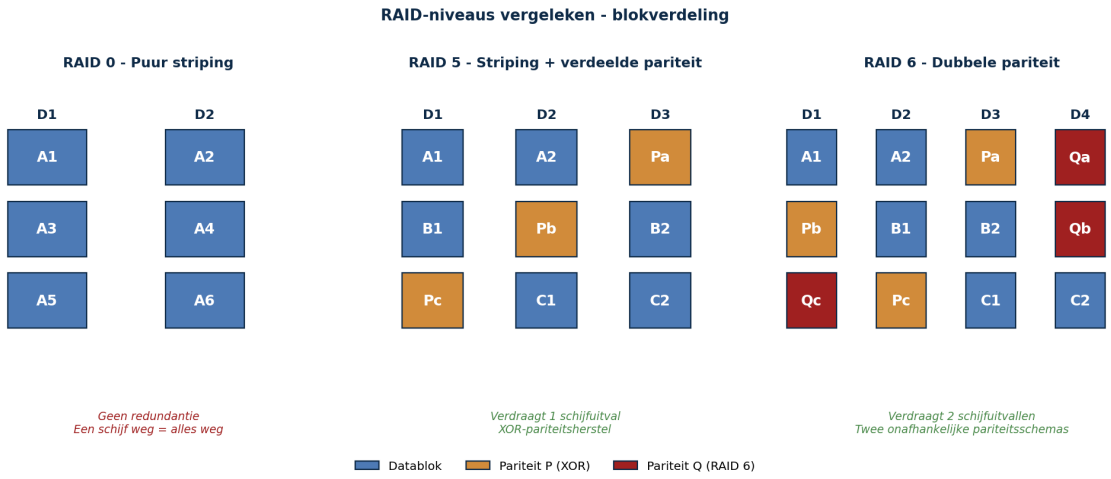
DEEL III — METHODEN

Hoofdstuk 11

RAID en geavanceerde opslag

11.1 Configuratie-overzicht

RAID combineert meerdere schijven voor performance, veerkracht, of beide. De gangbare niveaus in 2026:



Vergelijking RAID 0 / 5 / 6: datablok- en pariteitslayout.

Niveau	Beschrijving	Tolerantie	Gebruik
RAID 0	Puur striping, performance	Geen	Caches - NOOIT voor data
RAID 1	Mirroring	1 schijf	Kleine servers
RAID 5	Striping + verdeelde pariteit	1 schijf	NAS, MKB-servers - gangbaar
RAID 6	Striping + dubbele pariteit	2 schijven	Hoge-capaciteit opslag
RAID 10	Mirror van stripes	Tot N/2	Performance + redundantie
SHR	Synology Hybrid RAID	1 (SHR) of 2 (SHR-2)	Synology NAS

11.2 De gouden regel: imagen VOOR alles

De fatale valkuil in RAID-herstel is de **automatische rebuild** op een gedegradeerde array. Het probleem: de rebuild **schrijft massaal** op de resterende schijven. Als een andere schijf stilletjes stervende was, kan de extra belasting hem omkantelen.

Let op — Op een gedegradeerd RAID met belangrijke data: **stop de server, label elke schijf fysiek met zijn bay-positie, en image elke schijf individueel voor enige andere operatie**. Rebuilding gebeurt later, op de images, in een geisoleerde omgeving.

11.3 Software-reconstructie

Eenmaal elke schijf read-only geimaged, wordt de RAID virtueel gereconstrueerd met tools zoals R-Studio Network, UFS Explorer RAID, ReclaiMe Pro, of mdadm op Linux. De uitdaging is de exacte parameters te vinden:

- De **schijfvolgorde** in de stripe.
- De **stripe-grootte** (64 KB, 128 KB, 256 KB).
- Het **pariteits-schema** (left-symmetric, etc.).
- De initiele **offset**.
- De **pariteits-vertraging** op Dell PERC en HP Smart Array.

LABRAPPORT — DAFOTEC • RAID 5 Dell PowerEdge, 3 schijven in 'Foreign' staat (case #2)

Apparaat: RAID 5 / 6 schijven van 4 TB • **Doorlooptijd:** 48 uur (oproepdienst) • **Vast tarief:** 2.700 EUR (Franse markt)

Symptoom. Stroomonderbreking en spanningspiek. Bij herstart markeert de PERC H730-controller 3 schijven als "Foreign" en weigert de array te mounten. Auto-rebuild was gelukkig uitgeschakeld door de beheerder.

Interventie. Fysieke labeling van elke schijf in zijn bay. Forensisch klonen van elk van de 6 schijven met ddrescue en write blocker, naar identieke doelschijven. Virtuele reconstructie van XOR-pariteit zonder enige schrijfactie op de originelen. Identificatie van schijfvolgorde en pariteits-vertraging specifiek voor de PERC H730 via entropie-analyse.

Resultaat. 22 TB boekhoudkundige data intact hersteld. Bedrijfsactiviteit hervat binnen 48 uur.

Boekhoudkundig kantoor (38 medewerkers), regio Lyon - bedrijfsonderbreking vermeden. Case gepubliceerd op dafotec.fr.

11.4 Synology / QNAP NAS

Consumenten- en MKB-NAS gebruiken vaak moderne FS (Btrfs op Synology, ZFS op QNAP). Bij NAS-storing:

- Reset de NAS nooit — de RAID-configuratie zit in de metadata op de schijven.
- Extract de schijven met notatie van originele volgorde.
- Op Linux: mdadm --examine op elke schijf onthult de configuratie.
- UFS Explorer Professional en ReclaiMe Pro herkennen Synology en QNAP automatisch.

NAS en ransomware — Op moderne Synology DSM 7 NAS-units enables het Btrfs-bestandssysteem snapshots standaard. Bij ransomware-aanval is de typische procedure: 1) forensisch klonen van schijven, 2) read-only assemblage met mdadm --assemble --readonly, 3) mount met btrfs -o ro,recovery, 4) btrfs subvolume list -s om snapshots voor de aanval te identificeren, 5) extractie van schone data. Op veel eCh0raix, QlockerBunny en DeadBolt aanvallen vermijdt deze procedure elke losgeldbetaling.

11.5 Herstel via chip-off op NAS

Wanneer de schijven van een NAS zelf fysiek defect zijn (multi-disk failure na spanningspiek), moeten voorgaande technieken worden gecombineerd: herstel elke schijf individueel, reconstrueer dan virtueel de RAID.

11.6 Herstel op monolith-apparaten (microSD, all-in-one USB)

Monolith-apparaten zijn componenten waar NAND, controller en interface in dezelfde epoxyhars zijn ingebed: microSD, all-in-one USB 3.0-sticks. Wanneer het component fysiek beschadigd is (geoxideerde contacten, gekraste hars, verbrijzeld apparaat), kunnen noch de chips, noch de controller via klassieke middelen worden bereikt.

De hersteltechniek bestaat uit:

1. Abraden van de epoxyhars door laser of chemisch om de interne sporen bloot te leggen.
2. Identificeren onder microscoop van contactpunten die overeenkomen met NAND-datapinnen.
3. Microsolderen van extreem dunne koperdraden (0,02 mm) op deze punten.
4. Aansluiten op een universele NAND-programmer en raw dump uitvoeren zoals in klassieke chip-off.
5. Logisch reconstrueren zoals in 10.3.3.

Deze zeer technische procedure wordt door DAFOTEC publiek gedocumenteerd onder de naam *Spider Web*, verwijzend naar het web van fijne koperdraden dat eruit voortkomt onder de microscoop. Zeer weinig laboratoria in Frankrijk beheersen deze techniek.

LABRAPPORT — DAFOTEC • microSD-kaart uit DJI Mavic 3 drone (case #6)

Apparaat: microSD 256 GB UHS-II (monolith-apparaat) • **Doorlooptijd:** 4 dagen • **Vast tarief:** 320 EUR (Franse markt)

Symptoom. Drone gecrasht van ongeveer 40 meter hoogte. microSD-kaart niet herkend, contacten zichtbaar geoxideerd, componenthars gekraste langs de bovenrand.

Interventie. Spider Web techniek: laserabrasie van de epoxyhars aan de NAND-pinnen, identificatie van contactpunten onder microscoop, microsoldering van 28 koperdraden van 0,02 mm op de datapinnen. Raw dump op NAND-programmer, daarna logische reconstructie (descrambling, ECC, pagina-herassemblage).

Resultaat. 240 GB hersteld van 256 GB - 4 uur 20 minuten 4K architecturale verkennings-opnames. De ontbrekende 16 GB kwam overeen met fysiek verbrijzelde sectoren bij impact.

Professionele videograaf, regio Nice - commerciele opname gered. Case gepubliceerd op dafotec.fr.

Deel IV

Bijzondere gevallen

Drie domeinen waar algemene technieken op specifieke beperkingen stuiten: versleuteling, mobiele apparaten (smartphones, moderne Macs), en de juridische context.

DEEL IV — BIJZONDERE GEVALLEN

Hoofdstuk 12

Versleuteling en herstel

12.1 Een paradigmaverschuiving

Wanneer een apparaat onversleuteld is, is de data leesbaar door iedereen die de fysieke opslag bereikt. Wanneer een apparaat versleuteld is, is de data geen informatie meer; het is een reeks bits die niet te onderscheiden is van willekeurige ruis. Herstel wordt een cryptanalyse-probleem, wat in de praktijk betekent: **onmogelijk zonder de sleutel**.

12.2 BitLocker (Windows)

BitLocker versleutelt Windows-volumes met AES-128 of AES-256. De masterkey (FVEK) wordt beschermd door een of meerdere **protectors**:

- TPM (Trusted Platform Module): sleutel in de motherboard-module.
- Gebruikerswachtwoord.
- 48-cijferige herstelsleutel (opgeslagen in Microsoft-account / Azure AD).
- USB-sleutel, smartcard.

Zonder enige protector weerstaat correct geimplementeerde AES-128 of AES-256 alle bekende aanvallen. Geef op.

Goed systematisch spoor: de herstelsleutel opgeslagen in het Microsoft-account. Op te halen via account.microsoft.com of via de AD/Azure-beheerder.

12.3 FileVault (macOS)

FileVault 2 versleutelt het hele APFS-volume met AES-XTS. Op Apple Silicon Macs (M1 tot M4) is het standaard ingeschakeld en beheerd door de Secure Enclave.

Herstelpaden:

- Gebruikerswachtwoord.
- 24-tekens herstelsleutel (opgeslagen in iCloud bij activatie).
- Institutionele sleutel voor enterprise-Macs.

Zonder een van deze paden heeft chip-off geen interesse: alleen versleutelde data wordt verkregen.

12.4 LUKS (Linux)

LUKS (Linux Unified Key Setup) is de Linux-standaard. De LUKS-header bevat tot 8 passphrase-slots.

- Met bekende passphrase: cryptsetup open.
- Corrupte header maar backup (cryptsetup luksHeaderBackup): herstel.
- Zonder iets: Argon2/PBKDF2 + hoge kostfactor maken brute force onpraktisch op moderne passphrase.

Preventietip — Het backuppen van de LUKS-header bij installatie is een goede praktijk. Corruptie van de eerste sectoren zonder backup maakt het volume permanent onleesbaar.

12.5 Self-Encrypting Drives (SED, TCG Opal)

Hardwarematige versleuteling in de SSD-controller is steeds meer de norm. Het is:

- Altijd actief (controller decodeert met default-sleutel als geen wachtwoord is ingesteld).
- Activeerbaar via BIOS/UEFI (ATA-wachtwoord) of TCG Opal Manager-software.
- Direct wisbaar door *crypto erase* — vandaar dat SSD-verwijdering in seconden veilig is.

Verschillende SSDs hadden defecte Opal-implementaties (Crucial MX100/MX200, Samsung 840/850 EVO voor firmware EMT02B6Q) die omzeiling toelieten — maar erop rekenen is loterij spelen.

12.6 Ransomware: wat echt mogelijk is

Wanneer een werkstation of server wordt geraakt door moderne ransomware, worden gebruikersbestanden versleuteld met een sleutel (typisch AES) zelf versleuteld door de publieke sleutel van de aanvaller. Zonder de overeenkomstige private sleutel is decryptie wiskundig onmogelijk.

Paden om systematisch te onderzoeken voordat u in wanhoop verzinkt:

1. **Publieke decryptor?** Het *No More Ransom*-project (nomoreransom.org), gedragen door Europol, publiceert gratis tools voor varianten waarvan de sleutels zijn buitgemaakt. Meer dan 200 tools in 2026.
2. **Machine nog aan?** Als de aanval recent is, kan de AES-sleutel in klare tekst nog in het geheugen zitten. RAM-analyse met Volatility of DumpIt.
3. **Shadow Copies?** Op Windows kan vssadmin list shadows Shadow Copies onthullen die ransomware niet heeft kunnen verwijderen.
4. **Btrfs/ZFS snapshots op NAS?** De meeste NAS-ransomware versleutelt zichtbare bestanden maar vergeet read-only snapshots.
5. **Immutable of air-gapped backups?** Primaire vraag (hoofdstuk 17).
6. **Moet u betalen?** Complexe vraag. 64% van de slachtoffers weigerde in 2024. Betalen geeft geen garantie op decryptie.

Let op — Bewaar de versleutelde bestanden ook al kunt u ze vandaag niet ontsleutelen. Sleutels van historische ransomware (LockBit, Hive, REvil) worden regelmatig in beslag genomen door politie en maanden of jaren later gepubliceerd.

LABRAPPORT — DAFOTEC • Synology DS920+ NAS versleuteld door eCh0raix ransomware (case #4)

Apparaat: NAS RAID 5 / 4 schijven van 8 TB • **Doorlooptijd:** 7 dagen • **Vast tarief:** 1.800 EUR (Franse markt)

Symptoom. eCh0raix-aanval op een aan internet blootgestelde NAS. Alle gebruikersbestanden versleuteld met extensie .encrypt. Twee schijven tonen ook fouten op de RAID-controller.

Interventie. Forensisch klonen van alle 4 schijven met ddrescue. Read-only assemblage van het SHR Btrfs volume via mdadm. Analyse van Btrfs-snapshots: identificatie van de meest recente snapshot voor de aanval, gedateerd de vorige nacht. Extractie van het schone subvolume via btrfs send/receive naar schone opslag.

Resultaat. 24 TB hersteld via Btrfs-snapshot van D-1. Geen losgeld betaald.

E-commerce MKB (12 werknemers), regio Lille - productdatabase intact. Case gepubliceerd op dafotec.fr.

12.7 Casestudy — Maersk en NotPetya (juni 2017)

■ Maersk / NotPetya: backup gered door een stroomstoring

Op 27 juni 2017 werd de scheepvaartreus Maersk geraakt door **NotPetya**, destructieve malware vermomd als ransomware, verspreid via een gemanipuleerde update van de Oekraiense boekhoudsoftware M.E.Doc. In 7 minuten verspreidde de malware zich over het hele Maersk-netwerk: 45.000 tot 49.000 werkstations, 4.000 servers vernietigd, inclusief alle ~150 **Active Directory domain controllers**. NotPetya is niet omkeerbaar: de machines zijn dood.

Maersk had backups van individuele servers (3 tot 7 dagen oud), maar geen backups van domain controllers — de architectuur ging ervan uit dat de 150 controllers elkaar backupten via replicatie. Maar ze werden allemaal tegelijkertijd vernietigd. Zonder AD kan niets worden hersteld.

Redding: een domain controller in Ghana was **offline** op het moment van de aanval, vanwege een lokale stroomstoring. Hij had overleefd. Maersk liet hem fysiek verschepen (het netwerk was vernietigd) naar Londen waar het herstelcentrum was opgezet. Deze controller diende als basis om de hele infrastructuur te herbouwen.

Totaal: 10 dagen totale verlamming, geschat verlies van $250-300 miljoen voor Maersk. Wereldwijd kostte NotPetya ongeveer $10 miljard. Bronnen: Wired *The Untold Story of NotPetya* (2018); Control Engineering *Throwback Attack* (2025).

Les: online en synchroon onderling verbonden backups beschermen niet tegen een aanval die ze allemaal tegelijk vernietigt. Overleving kwam door geluk.

DEEL IV — BIJZONDERE GEVALLEN

Hoofdstuk 13

Mobiele apparaten en Apple Silicon

13.1 De context

Een moderne smartphone bevat typisch meer persoonlijke data dan een desktop. Maar het is ook een van de moeilijkste apparaten om te herstellen:

- Standaard versleuteling (iPhone sinds 2010; Android 6 sinds 2015 in de praktijk).
- Monolithische eMMC- of UFS-opslag.
- Sterke link met een cloud-account.

13.2 iPhone en iOS

Sinds iPhone 5s (2013) slaat de **Secure Enclave** sleutels op en past een strikt beleid toe op decryptie. Alle data op de NAND is versleuteld door een sleutel gebonden aan de passcode en een hardware-UID.

- Chip-off levert oninterpreteerbare versleutelde data.
- Professionele forensische tools (Cellebrite UFED, GrayKey, Magnet GrayKey) exploiteren niet-onthulde kwetsbaarheden in bepaalde iOS-versies.
- Voor particulieren: iTunes/Finder-backup of iCloud-backup.

13.3 Android

Meer heterogeen. Standaard versleuteling sinds Android 6, gebaseerd op de passcode en een hardware-keystore (**TEE**). Android 10+ gebruikt file-based encryption.

Tools:

- **Professionele forensische suites**: Cellebrite UFED, MSAB XRY, Oxygen Forensic Detective, Magnet AXIOM.
- **ADB**: op een ontgrendelde live telefoon met USB-debugging.
- **Download / EDL**-modus op sommige Qualcomm-chips — nu fabrikant-gesigneerd.

Voor een verloren vergrendelde Android blijft het meest praktische pad de **Google-backup**.

13.4 Fysiek vernietigde smartphones

Wanneer de smartphone fysiek vernietigd is, bestaan geavanceerde technieken maar vereisen een laboratorium:

- **Board-level micro-soldering**: reparatie van gesneden sporen, vervanging van defecte componenten.
- **Mobile CPU swap**: transplantatie van de processor (met Secure Enclave / TEE en dus de versleutelingssleutels) op een blanco donor-moederbord, met behoud van de cryptografische keten. Gestandaardiseerde procedure in laboratoria, publiek gedocumenteerd door DAFOTEC.

- **Directe NAND-lezing** op de gedesoldeerde eMMC- of UFS-chip — maar zonder Secure Enclave alleen versleutelde data.

LABRAPPORT — DAFOTEC • iPhone 15 Pro verbrijzeld door een tractor (case #5)

Apparaat: iPhone 15 Pro • **Doorlooptijd:** 10 dagen • **Vast tarief:** 380 EUR (Franse markt)

Symptoom. iPhone overreden door de wielen van een landbouwtractor. Chassis gebogen op 90 graden, moederbord transversaal in tweeen gebarsten, scherm verpulverd. Geen reactie op stroom.

Interventie. Forensisch microsolderen van het moederbord onder microscoop: herverbinding van gesneden sporen aan weerszijden van de breuk. Transplantatie van de Apple A17 Pro processor (mobile CPU swap, met Secure Enclave en dus de FileVault-sleutels van het apparaat) op een blanco donor-moederbord op BGA-station. Behoud van de cryptografische keten. Extractie van het UFS-image na boot in DFU-modus.

Resultaat. 100% van contacten, SMS, foto's, agenda en app-data (WhatsApp, banking) hersteld.

Boer, Normandie - professioneel adresboek gered. Case gepubliceerd op dafotec.fr.

13.5 Apple Silicon Macs: T2 en M1-M4

Op Apple Silicon Macs en oudere Intel Macs met T2-chip is de SSD **op het moederbord gesoldeerd** en zijn controller geintegreerd in de SoC. Drie gevolgen:

- Geen verwijderbare SSD — elke interventie vereist openen en werken op het moederbord.
- FileVault standaard actief, sleutel gebonden aan de Secure Enclave.
- Een board-level stroomstoring is voldoende om het hele apparaat onbruikbaar te maken.

Typische procedure om een Apple Silicon Mac met defect moederbord te herstellen waarvan de gebruiker het FileVault-wachtwoord kent:

1. Schemats en boardview-analyse om dode power rails te identificeren.
2. Component-niveau reparatie van doorgebrande MOSFETs en PMICs.
3. Indien moederbord te beschadigd: transplantatie van kritische componenten (SoC, gesoldeerde SSD-controller, NAND) op een donor-moederbord.
4. Lees de interne SSD via hardware DFU-interface.
5. Ontsleutel met het gebruikerswachtwoord.
6. Extract het image naar een nieuw apparaat.

LABRAPPORT — DAFOTEC • MacBook Pro M2, gesoldeerde SSD, macOS-update geblokkeerd (case #3)

Apparaat: MacBook Pro 14" M2 (2023) • **Doorlooptijd:** 5 dagen • **Vast tarief:** 480 EUR (Franse markt)

Symptoom. MacBook vastgelopen op het Apple-logo na een macOS 14.4-update. Recovery mode opstart onmogelijk. Geen standaard DFU-lezing. Gebruiker heeft het FileVault-wachtwoord.

Interventie. Extractie van het moederbord, boardview-analyse. Identificatie van een defecte power rail aan de gesoldeerde SSD-zijde. Directe lezing van Apple NAND-chips via proprietaire hardware DFU-interface na board-level reparatie. Decryptie via het door de klant verstrekte FileVault-wachtwoord.

Resultaat. 890 GB hersteld van 1 TB - volledige Lightroom-foto's, intacte Final Cut Pro-projecten, professionele documenten.

Onafhankelijke filmmaker, regio Bordeaux - 3 jaar rushes gered. Case gepubliceerd op dafotec.fr.

13.6 De rol van cloud-backups

Voor mobiele apparaten is dit bijna altijd het meest productieve pad. Herstel vanaf iCloud (Photos, contacten, mail, Drive, iOS-backups), Google (Photos, contacten, agenda, Drive, Android-backups), WhatsApp/Signal/Telegram.

DEEL IV — BIJZONDERE GEVALLEN

Hoofdstuk 14

Gerechtelijke forensiek

14.1 Het fundamentele verschil

Klassiek herstel heeft een eenvoudig doel: herstellen wat herstelbaar is. Gerechtelijke forensiek voegt een tweede toe: **een in de rechtbank toelaatbaar resultaat produceren**. Procedure wordt even belangrijk als techniek.

- Continue documentatie (*chain of custody*).
- Integriteitsverificatie door hash bij elke stap.
- Gebruik van write blockers.
- Reproduceerbaarheid: een andere expert moet dezelfde analyse kunnen herdoen.
- Erkende en gevalideerde tools.

14.2 ISO 27037: de referentiestandaard

ISO/IEC 27037:2012 definieert het internationale kader in vier fases:

1. **Identificatie**: lokaliseer apparaten met bewijs.
2. **Verzameling**: neem fysieke bezit op gedocumenteerde manier.
3. **Acquisitie**: creeer een geverifieerde forensische kopie.
4. **Bewaring**: handhaaf integriteit in de tijd, met gedocumenteerde chain of custody.

In Frankrijk werken gerechtelijke computer-experts binnen het strafrecht-kader. Inbeslagnames worden uitgevoerd door de Politie (cybercrime sub-directoraat) met expert-ondersteuning.

14.3 Chain of custody stap voor stap

Hier is een complete en concrete procedure:

1. **Ontvangstdocumentatie.** Hoge-resolutie foto's van alle hoeken. Notatie van fabrikant, model, serienummer, opgegeven capaciteit. Wegen indien relevant. Algemene fysieke toestand. Alle elementen in een receptierapport ondertekend door drager en ontvanger, gedateerd op de minuut.
2. **Labeling en verzegeling.** Aanbrengen van een genummerde verzegelde zak. Nummer getraceerd in een masterregister.
3. **Opslag.** Bewaring in een afgesloten kluis of kast met getraceerde toegang.
4. **Acquisitie-voorbereiding.** Verbreking van het zegel: verificatie dat het zegel intact is, foto, notatie in het masterregister.
5. **Aansluiting op het analyseststation.** Altijd via een hardware write blocker (Tableau, WiebeTech, Atola). Notatie van model en serienummer.
6. **Acquisitie.** Image-creatie in E01- of raw DD-formaat met FTK Imager, dc3dd, of Atola. Automatische berekening van MD5 + SHA1 (of SHA256). Hashes genoteerd in het rapport.

7. **Kruisverificatie.** Bereken een hash direct op de bron via de write blocker (read-only). Vergelijk met de image-hash. Beide moeten bit-voor-bit overeenkomen.
8. **Herverzegeling.** Onmiddellijke terugkeer van de bron naar zijn zak, herverzegeling, foto, register.
9. **Analyse.** Alle werk wordt exclusief op kopieen van het image gedaan. Elke gebruikte tool wordt genoteerd met zijn exacte versie. Elke manipulatie wordt gelogd.
10. **Rapport.** Beschrijving van het apparaat, complete procedure, hashes, tools, methodologie, conclusies, lijst van geproduceerde artefacten. Expert-handtekening en datum.

Waarom het cruciaal is — Een gebrekkige chain of custody (ongedocumenteerd verbroken zegel, ontbrekende of divergerende hash, onbedoelde schrijfactie op de bron, niet-geidentificeerde tool) kan voldoende zijn om alle conclusies ontoelaatbaar te maken — ongeacht de technische kwaliteit van de stroomafwaartse analyse.

14.4 Forensische referentietools

- **EnCase Forensic** (OpenText): historische suite.
- **FTK** (AccessData / Exterro). FTK Imager alleen is gratis.
- **X-Ways Forensics**: Europese referentie, licht en snel.
- **Magnet AXIOM**: focus op cloud, mobiel en browser-artefacten.
- **Belkasoft X**: zeer goed op mobiel en messaging.
- **The Sleuth Kit + Autopsy**: open source, gratis, ruimschoots voldoende voor veel zaken.

14.5 Windows-artefacten om te analyseren

- **Register** (NTUSER.DAT, SOFTWARE, SYSTEM, SAM): config, aangesloten USB, uitgevoerde programma's.
- **Prefetch**: spoor van uitgevoerde programma's.
- **ShellBags**: in Explorer bekeken mappen.
- **RecycleBin**: bestanden verwijderd via prullenbak.
- **$LogFile en $UsnJrnl**: NTFS-journaal.
- **Event Logs** (.evtx).
- **Browsers**: geschiedenis, cookies, cache, downloads.

Let op — *Nooit* de doelmachine booten op zijn originele OS. Elke boot wijzigt honderden bestanden, wat voldoende kan zijn om bewijs ongeldig te maken. Verwijder altijd de schijf of boot op een read-only forensische live distributie (CAINE, DEFT, Tsurugi Linux).

Deel V

Praktijk

Twee hoofdstukken om van theorie naar concrete keuzes te gaan.

DEEL V — PRAKTIJK

Hoofdstuk 15

Tools in 2026: een realistisch overzicht

15.1 Methode

Dit hoofdstuk lijst tools op zonder "score op 5" of gekwantificeerde "herstelpercentages" te geven. Wat volgt is een functionele beschrijving en eerlijke positionering.

15.2 Open source tools

ddrescue (GNU)

De onmisbare imaging-tool. Zie hoofdstuk 6.

TestDisk (CGSecurity)

Partitietabel-reparatie, verwijderde partitie-herstel.

PhotoRec (CGSecurity)

Handtekening-gebaseerd carving. Meer dan 480 formaten herkend. Cross-platform.

The Sleuth Kit + Autopsy

Complete forensische suite.

extundelete, ext4magic, debugfs

Het Linux-trio voor ext4.

Eric Zimmerman tools

Gratis Windows-suite: MFTECmd, RECmd, LECmd, JLECmd, PECmd, Timeline Explorer.

15.3 Consumenten- en MKB-commerciele tools

Disk Drill (CleverFiles)

Windows en macOS. Toegankelijke interface. Gratis versie beperkt tot 500 MB.

EaseUS Data Recovery Wizard

Zeer schoon, multi-FS, gratis versie tot 2 GB.

Recuva (CCleaner)

Gratis, eenvoudig. Geschikt voor recente accidentele verwijderingen op Windows.

Stellar Data Recovery

Volledig assortiment. Goede reputatie op Office en multimedia.

15.4 Professionele tools

R-Studio (R-Tools Technology)

Referentie voor IT-technici en kleine laboratoria. Zeer goed op NTFS, ext4, APFS, RAID.

UFS Explorer (SysDev Laboratories)

Uitstekend op geavanceerde formaten (APFS, ZFS, Btrfs, Synology/QNAP NAS, complexe RAID).

ReclaiMe en ReclaiMe Pro

Gespecialiseerd in RAID-reconstructie en proprietaire configuraties.

15.5 Gerechtelijke forensische tools

EnCase, FTK, X-Ways, Magnet AXIOM, Belkasoft X, Cellebrite UFED, Oxygen Forensic, MSAB XRY. Voorbehouden voor instellingen en gespecialiseerde ondernemingen.

15.6 Laboratorium hardware-platforms

- **PC-3000** (ACE Lab): de facto standaard.
- **DeepSpar / Atola**: gerichte alternatieven.

Volledige laboratoriumuitrusting vertegenwoordigt enkele tienduizenden euros.

15.7 Beslismatrix

Situatie	Eerste te proberen tools
Recent accidentele verwijdering op HDD	TestDisk + PhotoRec (gratis) of Disk Drill / EaseUS
Verwijdering op SSD (TRIM waarschijnlijk)	Recuva/EaseUS proberen; SSD losgekoppeld -> lab
RAW-volume (NTFS/exFAT corrupt)	TestDisk voor partitie, R-Studio of UFS Explorer voor FS
Synology/QNAP NAS uitgevallen	Schijven verwijderen, UFS Explorer Professional of ReclaiMe Pro
Gedegradeerd RAID 5	Eerst imagen, dan R-Studio Network of UFS Explorer RAID
Mac met FileVault, sleutel bekend	Boot in target disk modus; of R-Studio for Mac
Mac met FileVault, sleutel onbekend	Check iCloud (herstelsleutel); anders opgeven
Klikkende HDD	Onmiddellijk uitzetten -> lab (nooit zelf)
SSD niet gedetecteerd	Lab (JTAG / chip-off)
Apple Silicon Mac non-bootable, FileVault bekend	Lab (board-level + DFU-lezing)
Gerechtelijke zaak	FTK Imager (gratis) + Autopsy, of pro suite
Vergrendelde Android-telefoon	Google-backup; voor forensiek: Cellebrite, MSAB
Vergrendelde iPhone	iCloud-backup; voor forensiek: GrayKey
Synology NAS versleuteld door ransomware	Klonen + Btrfs-snapshot analyse (hfdst. 11)

DEEL V — PRAKTIJK

Hoofdstuk 16

Fatale valkuilen en stappenplannen

16.1 De zeven fouten die data doden

1. **Hersteltools installeren op het bronapparaat.** Installatie schrijft waar verwijderde bestanden zijn.
2. **Bestanden herstellen op het bronapparaat.** Variant even catastrofaal.
3. **Een SSD aan laten staan na het incident.** TRIM en GC gaan door.
4. **Windows automatic repair accepteren.** chkdsk /f, autorepair op een corrupt FS: Windows schrijft actief.
5. **Een HDD openen buiten een cleanroom.** Zie hoofdstuk 9.
6. **Een NAND-chip desolderen met een soldeerbout.** Zonder gekalibreerd rework-station wordt de chip vernietigd.
7. **Backups bewaren in dezelfde omgeving als productie.** Code Spaces case (hieronder). Moderne ransomware target toegankelijke backups.

16.2 Casestudy — Code Spaces (juni 2014)

■ Code Spaces: 12 uur van bedrijf naar weg

Code Spaces was een code-hostingplatform (Subversion en Git) met 7 jaar geschiedenis, gevestigd in het VK, volledig gehost op AWS.

Op 17 juni 2014 leed het bedrijf onder een DDoS-aanval gevolgd door een afpersingsboodschap, achtergelaten in de EC2-console. De aanvaller had toegang tot het AWS-paneel verkregen — via credential-compromittering, zonder MFA ingeschakeld.

Code Spaces weigerde te betalen. Maar de aanvaller had al verschillende accounts op de achtergrond aangemaakt. Toen hij besefte dat Code Spaces de controle probeerde terug te nemen, lanceerde hij een methodische verwijdering: **EBS-snapshots, S3-buckets, AMIs, EC2-instances, storage-instances**.

Het kritieke punt: *de backups zaten in hetzelfde AWS-account als productie*. Eenmaal de toegang verkregen, kon de aanvaller alles tegelijk verwijderen.

Op 18 juni 2014 — 12 uur na het begin van de aanval — kondigde Code Spaces de permanente staking van activiteit aan. Bronnen: Threatpost (juni 2014); InfoWorld (2014); Wiz-analyse (2023).

Lessen: (1) bewaar nooit backups in hetzelfde account/domein als productie; (2) MFA verplicht op alle cloud-managementaccounts; (3) principe van minste recht; (4) heb een getest incident response plan.

16.3 Vier stappenplannen

Scenario A — exFAT USB-stick per ongeluk geformatteerd

Symptomen: de stick lijkt leeg na een per ongeluk getriggerde snelle formattering. Gebruiker realiseert zich dit onmiddellijk.

Diagnose: logisch. Snelle formattering heeft FAT-tabel en boot sector overschreven, maar niet de dataclusters.

Aanbevolen pad:

1. Stick onmiddellijk loskoppelen.
2. Op een andere machine, image de stick: sudo ddrescue -f -n -d /dev/sdX stick.img stick.map.
3. Werk op de image. Run TestDisk erop: testdisk stick.img.
4. Als TestDisk het FS niet herbouwt, run PhotoRec op de image.
5. Herstel naar een doelmap **op een ander apparaat**.

Typische uitkomst: volledig herstel, vaak met intacte namen.

Scenario B — NVMe SSD, kritisch bestand 30 minuten geleden verwijderd

Symptomen: hele directory verwijderd op interne SSD. TRIM is standaard actief. Machine is nog aan en wordt gebruikt.

Diagnose: logisch op SSD met TRIM. Venster bijna gesloten.

Aanbevolen pad:

1. **Schakel de machine onmiddellijk uit** (fysieke knop, niet "afsluiten").
2. Verwijder de SSD. Als gesoldeerde SSD (ultrabook, Mac), zet niet weer aan — ga naar lab.
3. Voor verwijderbare SSD: aansluiten op andere machine via SATA-USB of NVMe-USB-adapter **zonder het FS in schrijfmodus te mounten**. Op Linux: sudo blockdev --setro /dev/sdX voor alles.
4. Image: sudo ddrescue -f -n -d /dev/sdX ssd.img ssd.map.
5. Op de image, probeer logisch herstel met R-Studio of TestDisk.

Typische uitkomst: random. Wees niet optimistisch op gezonde NVMe Samsung 980 Pro of WD SN850 SSDs.

Scenario C — Gedegradeerd RAID 5 na slechte manipulatie

Symptomen: op een Dell PowerEdge-server met 5 schijven van 4 TB in RAID 5, werd een schijf vorige week als "failed" gemarkeerd. De admin verving een schijf (mogelijk de verkeerde) en lanceerde een rebuild. De rebuild crashte halverwege en de controller toont nu twee "foreign" schijven.

Diagnose: RAID 5 in maximum gevaar. Typische lab-case.

Aanbevolen pad:

1. **Stop de server onmiddellijk**.
2. Label elke schijf fysiek: bay-positie (1, 2, 3, 4, 5), model, serienummer, datum.
3. Verwijder de schijven en image ze **individueel** op een aparte werkstation met write blockers.

4. Werk alleen op de images.
5. In-house met R-Studio Network / UFS Explorer Professional, of door een gespecialiseerd lab te bellen.

Scenario D — Synology NAS versleuteld door ransomware

Symptomen: alle NAS-bestanden verschijnen met vreemde extensie (.encrypt, .lockbit, enz.). Een README of HOWTODECRYPT bestand is aanwezig in de root.

Diagnose: NAS-ransomware (eCh0raix, QlockerBunny, DeadBolt en varianten). Btrfs-snapshots zijn waarschijnlijk intact als de NAS DSM 7+ draaide.

Aanbevolen pad:

1. **Isoleer de NAS onmiddellijk van het netwerk** (ethernet-kabel uitnemen).
2. Verwijder de schijven met notatie van volgorde.
3. Sluit de schijven aan op een dedicated Linux-werkstation, geisoleerd van internet.
4. Assembleer de RAID read-only: sudo mdadm --assemble --readonly /dev/md0 /dev/sd[abcd]3.
5. Mount Btrfs in recovery: sudo mount -t btrfs -o ro,recovery /dev/md0 /mnt/nas.
6. Lijst snapshots: sudo btrfs subvolume list -s /mnt/nas.
7. Identificeer de meest recente snapshot **voor** de aanval (D-1 of D-2).
8. Extract de bestanden uit deze snapshot naar nieuwe opslag.
9. Herstel de NAS op een nieuw OS en wijzig alle wachtwoorden.

Typische uitkomst: vaak 100% herstel, zonder losgeld te betalen. Anders check nomoreransom.org.

16.4 Wanneer weten te stoppen

Vier tekenen: fysiek beschadigd apparaat; meerdere mislukte pogingen; inzet groter dan pro-kosten; juridische inzet. In deze gevallen, overdragen.

Deel VI

Preventie

Het beste herstel is dat wat u nooit hoeft te doen.

DEEL VI — PREVENTIE

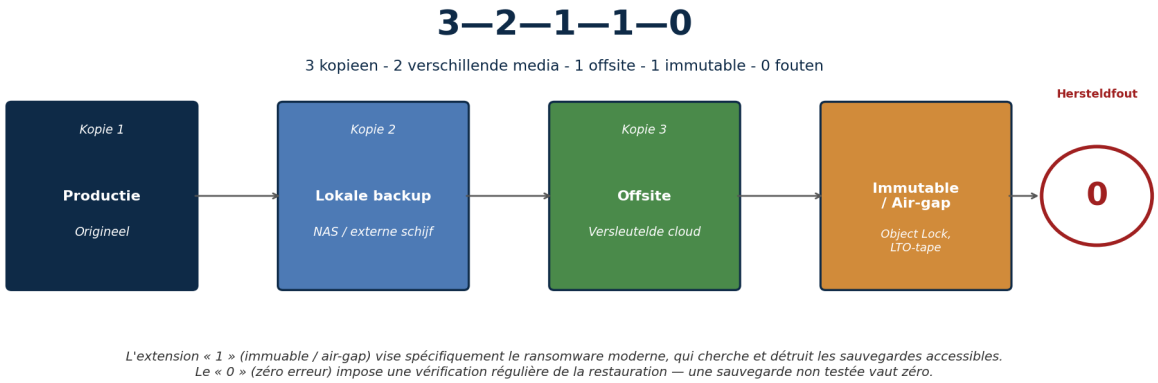
Hoofdstuk 17

Moderne back-upstrategieen

17.1 De 3-2-1-regel en zijn uitbreiding

De **3-2-1-regel** werd in 2005 geformuleerd door Peter Krogh, fotograaf, in *The DAM Book*. Hij komt neer op: **3** kopieen, **2** verschillende media, **1** offsite.

Twintig jaar later heeft de alomtegenwoordigheid van ransomware Veeam ertoe gebracht een uitbreiding **3-2-1-1-0** voor te stellen: **+1** immutable of air-gapped kopie, **+0** hersteltestfouten.



De 3-2-1-1-0-regel - vier kopieen, een immutable, nul hersteltestfouten.

Over de oorsprong — De 3-2-1-1-0-regel is Veeam-marketing, geen ANSI- of NIST-standaard. Dat doet niets af aan de inhoud: immutability en air-gap zijn essentieel geworden tegen moderne ransomware.

17.2 Immutability implementeren

- **S3 Object Lock** (AWS, Backblaze B2, Wasabi, MinIO).
- **Azure Blob immutability** en Google Cloud Storage retention policies.
- **Hardened Linux Repository** met chattr +i.
- **WORM** op tapes of optische schijven.
- **NAS snapshots** immutable: Synology SnapLock, QNAP WORM.

17.3 Air-gap

Een **air-gapped** apparaat is fysiek meestal losgekoppeld van het netwerk. Varianten:

- **LTO-tape** verwijderd uit robot en bewaard in kluis.

- **USB-schijf** alleen aangesloten voor backup, daarna opgeborgen.
- **Rotatie van meerdere externe schijven** met roterende offsite opslag.

17.4 Hersteltest-verificatie

De **0** van 3-2-1-1-0 is het meest verwaarloosde. Veel organisaties hebben backups die nooit zijn getest. Veelvoorkomende oorzaken:

- Stille corruptie (ongedetecteerde bit rot).
- Gebroken incrementele keten.
- Agent stil maanden geleden gecrashed.
- Applicatie die niet start vanaf backup.

Goede praktijk: **kwartaal** minimum hersteltest, **maandelijks** voor kritieke systemen.

17.5 Voor particulieren

1. Externe schijf 50-100 EUR voor Time Machine / File History.
2. Persoonlijke cloud: iCloud, Google One, Dropbox, OneDrive, Backblaze.
3. Voor echt onvervangbare bestanden, derde kopie op USB-stick bij familielid.
4. Jaarlijkse test: probeer een willekeurig bestand te herstellen vanaf elk van de drie kopieen.

17.6 Voor MKB

- Dagelijkse automatische backup (Veeam, Acronis, Datto, Synology Active Backup).
- Minstens een kopie in immutable cloud.
- Minstens een wekelijkse air-gapped kopie.
- MFA verplicht op alle admin-accounts.
- Gedocumenteerde maandelijkse hersteltest.
- Geschreven disaster recovery plan.
- Jaarlijkse oefening: fictief incident, kijk of het plan standhoudt.

DEEL VI — PREVENTIE

Hoofdstuk 18

Huidige grenzen in 2026

18.1 Wat definitief verloren is

1. **SSD met TRIM gepasseerd en GC voltooid.** Cellen in neutrale staat. Geen techniek herstelt.
2. **Door AES-256 versleutelde data zonder sleutel.** Wiskundig onhaalbaar met klassieke computers.
3. **HDD-platters met afgescheurde magnetische laag.** Informatie was in het metaal.
4. **Bestanden versleuteld door moderne ransomware zonder sleutel en zonder implementatiefout.**
5. **RAID 5 met meer dan een schijf defect, RAID 6 met meer dan twee.** Pariteit niet meer voldoende.
6. **Data overschreven door volledige herschrijving.** De mythe van magnetische remanence is ontkracht voor moderne schijven.

18.2 Wat moeilijk wordt

- **Mobiel herstel**: Secure Enclave, TEE, standaard versleuteling sluiten de deuren.
- **Klassieke SSDs**: betrouwbare TRIM, gegeneraliseerde hardwarematige versleuteling, verkort venster.
- **Cloud**: provider-zijde definitieve verwijdering is steeds rigider.

18.3 De laatste boodschap van dit hoofdstuk

Dataherstel is een echte, technisch complexe discipline die enorme vooruitgang heeft geboekt maar stuit op steeds strakkere fysieke en wiskundige grenzen. De methoden van hoofdstukken 6 tot 11 werken in de meerderheid van de gevallen, maar zijn bijna altijd afhankelijk van de tijd tussen het incident en de eerste goede beslissing.

De beste strategie blijft, niet verrassend, om niet te hoeven herstellen: preventie, echte geteste backup, operationele discipline wanneer er iets misgaat. Hoofdstuk 17 is in de praktijk het meest nuttige in het boek.

Deel VII

Horizon

Een vooruitkijkend hoofdstuk. Waar gaat de discipline de komende vijf tot tien jaar heen?

DEEL VII — HORIZON

Hoofdstuk 19

Horizon 2030: waar de discipline heen gaat

19.1 Aan de opslagkant: dichtheid, complexiteit

PLC NAND en verder

De eerste **PLC**-geheugens (5 bits per cel, 32 spanningsniveaus) werden tussen 2023 en 2025 aangekondigd door Solidigm en Kioxia. Progressieve commercialisatie over 2026-2028. Gevolgen voor herstel:

- Marges tussen spanningsniveaus nog krapper — onder 100 mV.
- Theoretische levensduur in vrije val (waarschijnlijk minder dan 150 P/E-cycli per cel).
- Ruwe lezing via chip-off moeilijker: vereist een ultra-precieze VNR, meerdere lezingen, en reconstructie van een nog zwaardere LDPC-pipeline.
- Praktisch gevolg: chip-off op PLC zal zeer waarschijnlijk voorbehouden zijn voor topklasse laboratoria.

HAMR op schaal

Seagate begon HAMR te commercialiseren op zijn Mozaic 3+ (30 TB en meer) in 2024. Toshiba en Western Digital zullen volgen. Tegen 2030 zullen 24 en 30 TB consumentenschijven HAMR zijn. Implicaties:

- Nog hogere lineaire dichtheid (boven 1,4 TB/platter).
- Complexere koppen (geintegreerde laser, puntig schrijven bij 450 graden C).
- Service Area nog kritischer.
- Voor herstel: geen fundamentele verandering van methode.

DNA-, holografische, 5D-optische opslag

Drie *archief*-opslagtechnologieen in R&D; sinds midden 2010. Geen heeft de algemene consumenten-commerciele fase bereikt in 2026, maar de beloftes zijn reeel:

- **DNA-opslag.** Microsoft, Twist Bioscience, Catalog. Codeert data in synthetische DNA-sequenties. Theoretische dichtheid in de orde van petabyte per gram, levensduur van duizenden jaren.
- **Holografische opslag** (HVD). Meerdere malen aangekondigd sinds 2008. Nog niet algemeen in 2026.
- **5D-optisch / Superman memory crystal** (Universiteit van Southampton). Glas genanostructureerd door femtoseconde-laser. Experimentele capaciteit van 360 TB op een schijf, geschatte levensduur van 13,8 miljard jaar.

Voor de dataherstel-specialist: deze technologieen zullen, wanneer ze arriveren, radicaal nieuwe problemen stellen. DNA-data lezen over 50 jaar zonder de originele sequencer? Het is niet meer hetzelfde vak.

19.2 Over methoden: AI en automatisering

AI-ondersteund carving

Verschillende forensische uitgevers hebben machine learning modules aangekondigd tussen 2023 en 2025:

- **Magnet AXIOM AI** (sinds 2024): automatische classificatie van potentieel illegale afbeeldingen, gezichtsdetectie, audio-transcriptie.
- **Belkasoft X AI** (sinds 2024): reassemblage-modules voor afbeeldingsfragmenten, detectie van AI-gegenereerde content.
- **Cellebrite AI Reveal** (aangekondigd 2025): automatische conversatie-samenvatting in smartphone-extracties.

Realistische beloftes: ja, deze benaderingen versnellen post-extractie-classificatie op grote volumes. Echte grenzen: geen werkt wonderen in de low-level carving-fase. AI helpt downstream, niet upstream.

ML-ondersteunde FTL-reconstructie

Sommige academische publicaties (USENIX, FAST 2023-2025) verkennen het gebruik van neurale netwerken om de scrambling-polynoom en ECC-pipeline van een SSD-controller te identificeren. Nog experimenteel; te volgen over 3-5 jaar.

19.3 Over cryptografie: post-quantum

NIST finaliseerde in 2024 de eerste post-quantum standaardisaties (CRYSTALS-Kyber voor key exchange, CRYSTALS-Dilithium voor handtekening, SPHINCS+ voor hashing). Implicaties voor herstel:

- AES-256 blijft robuust tegen Grover (reduceert effectieve beveiliging van 256 naar 128 bits, blijft onoplosbaar). AES-128 wordt theoretisch breekbaar maar niet in praktijk.
- Post-quantum vervangingen voor hardwarematige versleuteling (TCG Opal v2.x met post-quantum algo) zullen waarschijnlijk vanaf 2028-2030 arriveren.
- Implementatiefouten in deze nieuwe algoritmen — zoals gebeurde met sommige vroege Opal-implementaties — zullen tijdelijk onverwachte herstelvensters heropenen. Volg CVE/CERT-meldingen.

19.4 Over juridische en regelgevende aspecten

- **NIS2** (Network and Information Security Directive 2, EU) legt sinds oktober 2024 versterkte verplichtingen op voor incidentbeheer, backup en bedrijfscontinuiteit. Herstel wordt een regelgevingspunt.
- **DORA** (Digital Operational Resilience Act) voor de Europese financiele sector, van toepassing sinds januari 2025. Strikte eisen voor disaster recovery tests.
- **AVG/GDPR**: jurisprudentie over het bewaren van herstelkopieen wordt verfijnd. Serieuze laboratoria hebben de vernietiging van tijdelijke kopieen na teruggave aan de klant gecontractualiseerd.

19.5 Over economie

Drie trends:

- **Publieke prijzen** worden de norm — vijftien jaar geleden publiceerde bijna geen lab zijn prijzen. In 2026 publiceert DAFOTEC een complete prijslijst, en verschillende Franse laboratoria volgen.
- **Betaling bij resultaat** wordt standaard. Marktaanvaarding dat een klant niet betaalt als niets is hersteld.
- **Validatie voor betaling** (VeriFiles bij DAFOTEC, equivalenten bij andere labs) wordt een steeds explicieter klantverwachting.

19.6 Over opleiding

Dataherstel blijft een vak zonder diploma-curriculum. Opleiding gebeurt via stage in laboratoria en uitgevers-certificeringen (ACE Lab Certified, EnCase Certified Examiner, GCFE, CFCE). Tegen 2030 zouden dedicated modules kunnen ontstaan in cybersecurity-masters — sommige Franse universiteiten experimenteren hiermee sinds 2023 (Lille, Rennes, Compiegne, Lyon Master 2 Cyber-programma's).

19.7 Het vak verdwijnt niet

Een terugkerende vrees: met cloud, gegeneraliseerde backups en standaard versleuteling, is dataherstel een toekomstbestendig vak of een stervend?

Drie elementen wijzen erop dat het vak niet verdwijnt:

1. Het totale wereldwijd geproduceerde opslagvolume groeit exponentieel. Zelfs als een groeiend deel versleuteld of geback-uped is, neemt het residuele onbeschermde volume in absolute waarde toe.
2. Hardwarestoringen blijven onvermijdelijk (HDD AFR ~1,3% per jaar, eindige SSD-levensduur). Volumes groeien, herstelbehoeften ook.
3. Regelgevingsvereisten (NIS2, DORA, ISO 27001, AVG/GDPR) eisen steeds rigoureuzere forensische analyses en gedocumenteerde herstellingen.

Wat verandert: het vak wordt technischer (meer fysica, geavanceerdere elektronica, meer reverse engineering), gestandaardiseerder (chain of custody, compliance), en geconcentreerder (laboratoria die moderne zaken tot het einde kunnen behandelen zijn weinig). De discipline verdwijnt niet. Ze wordt professioneler.

Bijlagen

Quick reference

Vijf bijlagen: commando- en Python-script-referentie, verklarende woordenlijst, complete bibliografie, "Over DAFOTEC"-pagina, en thematische index.

BIJLAGEN

Hoofdstuk A

Commando- en script-referentie

A.1 Apparaatidentificatie

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

# macOS
$ diskutil list

# Windows (PowerShell)
PS> Get-PhysicalDisk
```

A.2 ddrescue imaging

```
# Eerste snelle pass
$ sudo ddrescue -f -n -d /dev/sdX image.img image.map

# Tweede pass met retry
$ sudo ddrescue -f -d -r3 /dev/sdX image.img image.map

# Omgekeerde pass voor zware gevallen
$ sudo ddrescue -f -d -R -r3 /dev/sdX image.img image.map

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

A.3 Image read-only mounten

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

# Mount volgens FS
$ sudo mount -o ro,noload /dev/loop0p1 /mnt/recovery # ext4
$ sudo mount -t ntfs-3g -o ro,norecover /dev/loop0p1 /mnt/recovery
$ sudo mount -o ro /dev/loop0p1 /mnt/recovery # FAT/exFAT
```

A.4 Integriteitshashes

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

$ b3sum image.img # BLAKE3 is sneller voor zeer grote bestanden
```


A.5 NTFS-analyse

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

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

A.6 ext4-analyse

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

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

A.7 Linux RAID (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 en 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 /herstel
```

A.9 TRIM-verificatie

```
# 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 RAM-capture (live forensics)

```
# Windows: DumpIt
C:\> DumpIt.exe

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

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


A.11 Python-script: ddrescue mapfile parser

Klein hulpprogramma dat de mapfile van een ddrescue-sessie parseert en statistieken toont per blokcategorie:

```
#!/usr/bin/env python3
"""parse_ddrescue_mapfile.py - Statistieken voor een ddrescue mapfile."""
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'Totaal: {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} %)')
```

A.12 Python-script: verwijderde MFT-entries extraheren

Kleine pedagogische parser die een geextraheerd $MFT-bestand leest en als verwijderd gemarkeerde entries lijst:

```
#!/usr/bin/env python3
"""parse_mft_deleted.py - Lijst verwijderde MFT-entries."""
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):
name = find_file_name(data)
if name:
deleted.append((record_idx, name))
record_idx += 1
return deleted

def find_file_name(record):
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:
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}')
```

Disclaimer — Deze scripts zijn pedagogisch en minimaal. Voor serieus gebruik, geef de voorkeur aan MFTECmd (Zimmerman) en de Sleuth Kit-suite.

BIJLAGEN

Hoofdstuk B

Verklarende woordenlijst

AES — Advanced Encryption Standard. Symmetrisch versleutelingsalgoritme. AES-128 en AES-256 weerstaan alle bekende aanvallen met klassieke middelen.

AFR — Annualized Failure Rate van een schijvenvloot.

Air-gap — Fysieke loskoppeling van een systeem van het netwerk.

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

BGA — Ball Grid Array. Behuizing met rooster soldeerballen onder de component.

Btrfs — Linux B-tree file system. Copy-on-write met snapshots en checksums.

Carving — Reconstructie van bestanden via binaire handtekeningen, zonder FS-structuren.

Chain of custody — Continue documentatie van behandeling van digitaal bewijs.

Charge trap (CTF) — Moderne NAND-cel-architectuur waar lading in een isolator wordt gevangen, robuuster dan floating gate. Massaal aangenomen sinds 2017.

Chip-off — Fysiek desolderen van een NAND-chip om onafhankelijk van zijn controller te lezen.

CMR — Conventional Magnetic Recording. HDD-modus met niet-overlappende sporen.

Copy-on-write — Elke wijziging schrijft elders en werkt pointers bij. Gebruikt door APFS, Btrfs, ZFS.

CPU Swap (DAFOTEC-methode) — Transplantatie van een smartphone-processor op een donor-moederbord, met behoud van Secure Enclave / TEE. Publiek gedocumenteerd door DAFOTEC.

DBIR — Data Breach Investigations Report. Jaarlijks Verizon-rapport sinds 2008.

ddrescue — GNU ddrescue. Bit-voor-bit imaging-tool tolerant aan fouten.

DRAT / DZAT — Deterministic Read After Trim / Deterministic Zero After Trim. SSD-garanties.

ECC — Error-Correcting Code. Correctiecodes toegepast door de SSD-controller op elke NAND-pagina.

eMMC — Embedded MultiMediaCard. Flash-geheugen met geintegreerde controller, voor low/mid-range smartphones.

ext4 — Standaard Linux-bestandssysteem sinds 2008.

FileVault — macOS-volumeversleuteling. Beheerd door de Secure Enclave op Apple Silicon Macs.

FTL — Flash Translation Layer. Laag in de SSD-controller die logische LBAs op fysieke NAND-paginas mapt.

Garbage collection (GC) — Achtergrondproces van de SSD-controller dat blokken gemarkeerd als vrij fysiek wist.

HSA-transplantatie — Head Stack Assembly-transplantatie. Overdracht van complete kop/arm-assemblage van twee-donor-schijf naar ontvanger, met sub-micron uitlijning onder 0,3 micron.

HAMR — Heat-Assisted Magnetic Recording. HDD-technologie die magnetische laag tijdens schrijven verhit per laser. Gecommercialiseerd sinds 2024.

HDD — Hard Disk Drive. Mechanische magnetische schijf.

Imaging — Creatie van een bit-voor-bit kopie van een apparaat naar een imagebestand.

ISO 14644-1 — Internationale norm voor cleanroom-klassen per deeltjesconcentratie.

ISO 27037 — Internationale norm voor verzameling en bewaring van digitaal bewijs.

JTAG / ISP — Intern debugprotocol blootgesteld door SSD-controllers. Geexploiteerd bij niet-destructief herstel.

LBA — Logical Block Address blootgesteld door de SATA/NVMe-interface.

LDPC — Low-Density Parity-Check. Foutcorrigerende code gebruikt door moderne SSD-controllers.

LUKS — Linux Unified Key Setup. Standaard Linux-volumeversleuteling.

Mapfile — Map-bestand gebruikt door ddrescue.

MFT — Master File Table. Centrale structuur van NTFS.

NAND flash — Floating-gate of charge-trap geheugen, technologie onder alle SSDs, eMMC, UFS, microSD, USB-sticks.

NTFS — New Technology File System. Windows-FS sinds NT.

Over-provisioning — NAND-ruimte gereserveerd door de SSD-controller, onzichtbaar voor de gebruiker.

PCB — Printed Circuit Board. Externe printplaat van een HDD of SSD.

PC-3000 — ACE Lab hardwareplatform, de facto standaard voor professioneel herstel.

PLC — Penta-Level Cell. 5 bits per cel NAND-geheugen, 32 spanningsniveaus.

PMR — Perpendicular Magnetic Recording. HDD-modus gegeneraliseerd sinds 2005.

RAID — Redundant Array of Independent Disks. Combinatie van meerdere schijven voor performance of veerkracht.

Ransomware — Kwaadaardige software die bestanden versleutelt en losgeld eist.

Read-retry — NAND-leestechniek die spanningsdrempels verschuift om een pagina te herstellen die de initiele lezing niet kon decoderen.

Reverse FTL — Software-reconstructie van de LBA-NAND mappingtabel van een SSD met defecte controller, vanuit metadata in NAND-paginas.

Cleanroom — Gecontroleerde atmosfeer-kamer gedefinieerd door ISO 14644-1. Voor HDD-herstel: ISO klasse 5.

Secure Enclave — Apple security coprocessor (iPhone 5s+, Mac T2, Apple Silicon) die cryptografische sleutels beheert.

SED — Self-Encrypting Drive. SSD die automatisch versleutelt via zijn controller, TCG Opal-standaard.

Service Area (SA) — Gereserveerde zone op HDD-platters, onzichtbaar voor het OS, met meer dan honderd firmwaremodules (P-list, G-list, translator, adaptives).

SMR — Shingled Magnetic Recording. HDD-modus met gedeeltelijk overlappende sporen.

Snapshot — Momentopname van een volume tegen bijna-nul kosten op copy-on-write FS.

Spider Web (DAFOTEC-methode) — NAND-extractieprocedure op monolith-apparaten (microSD, all-in-one USB). Laserabrasie van de hars en microsoldering van 15 tot 30 fijne koperdraden. Publiek gedocumenteerd door DAFOTEC.

TCG Opal — Trusted Computing Group standaard voor hardwarematige SSD-versleuteling.

TEE — Trusted Execution Environment. Android security coprocessor (equivalent van Secure Enclave).

Translator — HDD-firmwaremodule die LBA omzet naar fysieke coordinaten. Module 028 op WD ROYL.

TRIM — ATA-commando (DATA SET MANAGEMENT) of NVMe (DEALLOCATE) dat de SSD-controller informeert over LBAs vrijgemaakt OS-zijde.

UFS — Universal Flash Storage. eMMC-opvolger voor high-end smartphones.

VeriFiles (DAFOTEC-service) — Service: de klant beoordeelt de complete lijst van herstelbare bestanden voor enige betaling.

Wear leveling — SSD-strategie die schrijfacties over alle NAND-cellen verdeelt.

WORM — Write Once Read Many. Immutable opslag.

Write blocker — Hardware- of software-apparaat dat alle schrijfacties naar een apparaat blokkeert.

ZFS — Sun Microsystems file system (2006), nu OpenZFS. Copy-on-write, checksums, self-healing.

BIJLAGEN

Hoofdstuk C

Bibliografie

Publieke bronnen daadwerkelijk geraadpleegd voor dit handboek (mei 2026). Vereenvoudigde URLs.

Sectorrapporten

Verizon Business	2025 Data Breach Investigations Report. April 2025.	verizon.com/about/news/2025-data-breach-investigations-report
Backblaze	Drive Stats for 2025. Februari 2026.	backblaze.com/blog/backblaze-drive-stats-for-2025/
IBM Security	Cost of a Data Breach Report 2024.	ibm.com/reports/data-breach
ENISA	Threat Landscape 2024.	enisa.europa.eu/topics/threat-risk-management/threats-and-trends/

Normen

ISO	ISO 14644-1:2015 - Cleanrooms classificatie.	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/

Europese regelgeving

EU	NIS2 Directive (Directive 2022/2555).	eur-lex.europa.eu/eli/dir/2022/2555/oj
EU	DORA Regulation (Regulation 2022/2554).	eur-lex.europa.eu/eli/reg/2022/2554/oj
EU	GDPR (Regulation 2016/679).	eur-lex.europa.eu/eli/reg/2016/679/oj

Cleanroom en HDD-herstel

DriveSavers	Certified ISO Class 5 Cleanroom.	drivesaversdatarecovery.com/
Rossmann Group	CMR vs SMR: How Recording Technology Affects Recovery.	rossmanngroup.com/
ACE Lab	PC-3000 publieke documentatie HDD/SSD modules.	acelab.eu.com/

SSD, NAND, TRIM, FTL

Rossmann Group	What TRIM Does and Why It Destroys Data.	rossmanngroup.com/
Seagate	What Are SSD TRIM and Garbage Collection?	seagate.com/blog/
Kingston	The Importance of Garbage Collection and TRIM.	kingston.com/en/blog/
Belkasoft / Forensic Focus	Recovering Evidence from SSD Drives.	forensicfocus.com/

Bestandssystemen

Sygnia	Forensic Value of MFT Slack Space. 2025.	sygnia.co/blog/
Brian Carrier	File System Forensic Analysis (referentieboek).	sciencedirect.com/

Tools

GNU	GNU ddrescue manual.	gnu.org/software/ddrescue/
CGSecurity	TestDisk en PhotoRec.	cgsecurity.org/wiki/TestDisk
Sleuth Kit	TSK en Autopsy.	sleuthkit.org/
Eric Zimmerman	Forensische tools.	ericzimmerman.github.io/
SANS Institute	DFIR papers en posters.	sans.org/white-papers/

Backup

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/

Historische casestudies

Wired	The Untold Story of NotPetya. 2018.	wired.com/story/notpetya-cyberattack/
Threatpost	Code Spaces Out of Business. Juni 2014.	threatpost.com/
InfoWorld	Murder in the Amazon cloud. 2014.	infoworld.com/
breaches.cloud / Wiz	Codespaces (2014).	breaches.cloud/incidents/codespaces/

DAFOTEC-bronnen

DAFOTEC	Officiele site: prijzen, technische expertise, echte casestudies, institutionele klanten.	dafotec.fr
DAFOTEC Belgie	Belgische versie van het laboratorium.	dafotec.be

BIJLAGEN

Hoofdstuk D

Over DAFOTEC

DAFOTEC is een Frans dataherstel-laboratorium opgericht in Roubaix in 2004. Dit handboek werd geschreven door Mhessan Kouassi, senior expert bij DAFOTEC sinds de oprichting, voortbouwend op 22 jaar veldpraktijk en meer dan 120.000 behandelde cases.

Identiteit

- **Laboratorium**: 59 Bis rue du Curoir, CS 40082, 59052 Roubaix Cedex (Frankrijk).
- **Sites**: dafotec.fr (Frankrijk) en dafotec.be (Belgie).
- **Leeftijd**: 22 jaar (2004 - 2026).
- **Behandeld volume**: meer dan 120.000 cases sinds 2004.
- **Dekking**: 36 inzamelpunten in Frankrijk, nationale ophaalservice, enkel analyse-laboratorium in Roubaix.

Certificeringen en compliance

- **ISO 5 cleanroom** (ISO 14644-1-norm) in Roubaix.
- **AVG/GDPR**-conformiteit voor de behandeling van persoonsgegevens.
- **ISO 27001**-conformiteit voor informatiebeveiliging.
- Behandeling van gevoelige apparaten op een fysiek van het internet geisoleerd netwerk (**air gapped**).

Institutionele klanten

DAFOTEC wordt regelmatig ingeschakeld door Franse publieke organisaties en wetenschappelijke instellingen voor het behandelen van defecte apparaten, onder geheimhoudingsovereenkomst (NDA). Klanten genoemd met hun toestemming:

- Franse Nationale Politie (Gendarmerie Nationale)
- Universitair Medisch Centrum Tourcoing
- CNRS (Frans Nationaal Centrum voor Wetenschappelijk Onderzoek)
- INSERM (Frans Nationaal Instituut voor Gezondheid en Medisch Onderzoek)
- Franse universiteiten

Businessmodel

- **Gratis diagnose** binnen 24 uur in het laboratorium.
- **Betaling bij resultaat**: het herstel vaste tarief wordt alleen in rekening gebracht bij succes. Bij mislukking is alleen een reconditionerings- en teruggavevergoeding van 25 EUR verschuldigd.

- **VeriFiles-service**: de complete lijst van herstelbare bestanden wordt aan de klant verstrekt *voor enige betaling*. De klant valideert deze lijst en beslist dan om de offerte zonder kosten te aanvaarden of weigeren.
- **Publieke prijzen**: 300 EUR voor een harde schijf, 400 EUR voor een SSD, 300 EUR voor een smartphone, 550 EUR per schijf voor een NAS, 700 EUR per schijf voor een RAID. Tot 950 EUR voor de meest complexe storingen. Prijzen weerspiegelen de Franse markt.

Onafhankelijke beoordelingen

4,9/5 op 797 geverifieerde Ekomi-beoordelingen op publicatiedatum van dit handboek (mei 2026).

Waarom dit handboek gratis is

Dit boek wordt gratis verspreid onder de Creative Commons BY-NC-ND 4.0-licentie, downloadbaar zonder registratie via dafotec.fr en dafotec.be.

De reden is consistent met de redactionele missie van het handboek: desinformatie in de dataherstel-sector verminderen; particulieren, MKB en administraties redden van verkeerde eerste beslissingen die herstel onmogelijk maken; technici en forensische studenten voorzien van een solide en gesourcede referentie.

DAFOTEC is een commercieel laboratorium, maar de inspanning van popularisatie en technische transparantie heeft op zich waarde. Als dit handboek een slechte manipulatie voorkomt, is het schrijven gerechtvaardigd.

Distributielicentie

Creative Commons Naamsvermelding — NietCommercieel — GeenAfgeleideWerken 4.0 Internationaal (CC BY-NC-ND 4.0).

U mag:

- **Delen** — het materiaal kopieren en herverdelen in elk medium of formaat.

Onder de volgende voorwaarden:

- **Naamsvermelding** — u moet passende krediet geven aan DAFOTEC, een link naar de licentie verstrekken, en aangeven of wijzigingen zijn aangebracht.
- **NietCommercieel** — u mag het materiaal niet voor commerciele doeleinden gebruiken.
- **GeenAfgeleideWerken** — als u het materiaal remixt, transformeert of erop voortbouwt, mag u het gewijzigde materiaal niet verspreiden.

Einde van het handboek. Mei 2026.
DAFOTEC — Roubaix — sinds 2004.

BIJLAGEN

Hoofdstuk E

Thematische index

Alfabetische index van de belangrijkste technische termen in het handboek, met paginaverwijzingen. Voor exacte definities, zie ook bijlage B (Woordenlijst).

A

B

C

D

E

F

G

H

I

J

L

M

N

P

R

S

T

U

V

W

Z