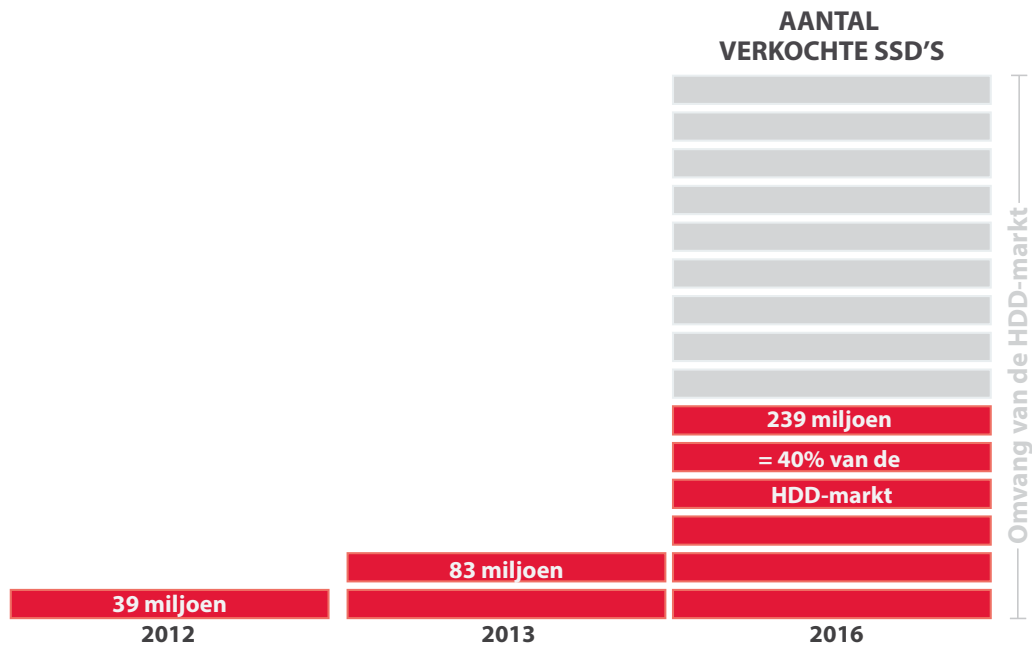


Uitdagingen en oplossingen voor het effectief wissen van SSD-gegevens

Inhoudsopgave

Inleiding	3
De eenvoud en complexiteit van SSD's.....	4
Op de gebruikelijke manier wissen levert gevaar op voor SSD's	5
Externe factoren die het wissen van SSD's compliceren	6
Gebrek aan standaardisatie door OEM's	6
Toename in de wetgeving voor gegevensbescherming en standaarden	6
De belangrijkste eisen voor het veilig wissen van SSD's.....	7
Tests en verificatie door derden.....	7
Verkrijgen van een standaard voor het wissen van SSD's	8
Verwijderen van blokkerende beveiligingen	8
Samenwerking leverancier-OEM	9
Samenvatting: Professionele tools omzeilen de barrières voor het wissen van een SSD.	10
Verwijzingen	11



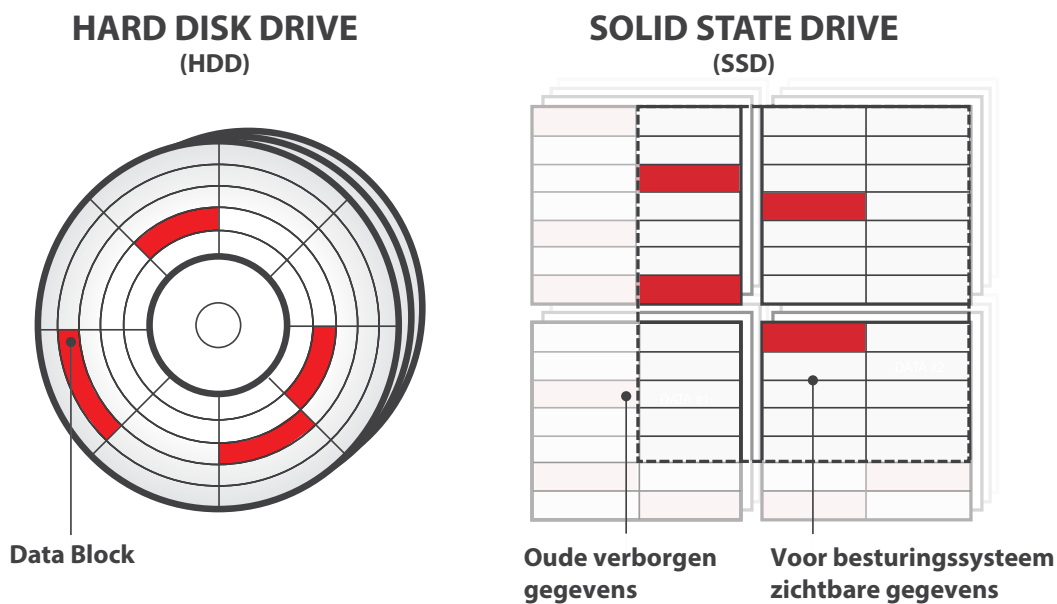
Inleiding

De Solid State Drive (SSD), een veelzijdig en betrouwbaar apparaat voor massaopslag, is gegroeid van een bijzonder product tot een product voor normaal gebruik door consumenten en bedrijven, en fungeert als rechtstreekse vervanging voor de traditionele harde schijf (HDD). Aangestuurd door de verbeterde prestaties van de SSD, de betrouwbaarheid en de kleine omvang met grote dichtheid, wordt voorspeld dat in 2013 zo'n 83 miljoen SSD-eenheden zullen worden geleverd – een toename van meer dan 100% ten opzichte van het aantal in 2012 verkochte schijven.¹

Naarmate SSD's populairder worden, worden managers van IT-hardware en specialisten voor het verwijderen van IT-hardware (ITAD's) geconfronteerd met verschillende uitdagingen bij het veilig wissen van gegevens van SSD's die gereserveerd zijn voor pensionering, hergebruik of verwijderen. In tegenstelling tot de mechanische tegenhanger de vaste schijf (HDD), maakt een SSD gebruik van het flash-geheugen dat het volledig verwijderen van gegevens met methoden voor HDD's compliceert.

En omdat de SSD-markt zo snel is gegroeid, is hij verzadigd door een groot aantal leveranciers, elk met hun eigen aanbod aan SSD-modellen die vaak verschillen op het punt van de operationele processen. Dit gebrek aan standaardisatie compliceert het wissen nog meer, met name gezien de snelheid waarmee SSD's nog steeds verder worden ontwikkeld.

Voor IT-beheerders in bedrijven, en voor externe recyclers en de ITAD's die hen ondersteunen, is het belangrijk om de SSD-technologie te begrijpen, waarom het wissen van SSD's zo'n uitdaging is, en het belang van de keuze van een effectief wisproduct met gedetailleerde mogelijkheden voor rapportage. Effectieve en efficiënte software voor het wissen van gegevens is ontwikkeld door een leverancier die technieken kan toepassen welke exclusief zijn ontworpen voor het wissen van SSD's, en die verificatie van derden heeft gekregen voor de effectiviteit van de software en die toegang heeft tot belangrijke R&D-bronnen om de ontwikkeling van de technologie bij te houden. Deze expertise voorkomt dat vals positieve meldingen optreden als gevolg van het gebruik van een niet-effectieve technologie of proces, wat een kostbare inbreuk op gegevens kan veroorzaken.



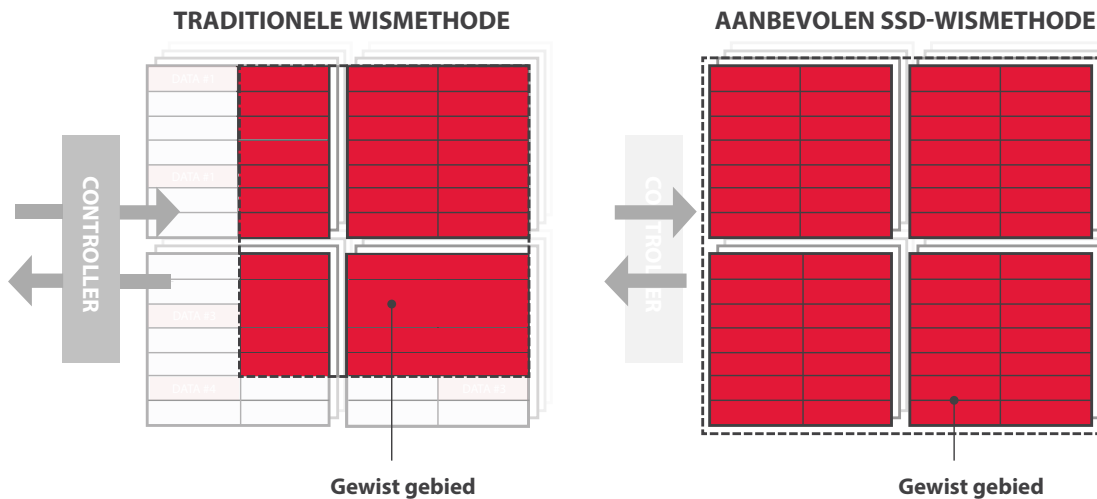
De eenvoud en complexiteit van SSD's

Vanuit fysiek oogpunt gezien zijn SSD's eenvoudig, omdat ze niet beschikken over bewegende onderdelen, in tegenstelling tot elektromechanische HDD's, die draaiende schijven en beweegbare lees/schrijfkoppen bevatten. Hiermee vergeleken zijn SSD's kleiner, stiller, sneller en minder gevoelig voor fysieke schokken. SSD's zijn ongeveer half zo groot als een harde schijf, ze wegen maar de helft daarvan en ze gebruiken de helft van het vermogen, zodat ze uitstekend geschikt zijn voor datacentra en andere omgevingen voor massa-opslag.

Vanuit een ander oogpunt gezien, worden SSD's steeds complexer. Flash-geheugen, gelijkwaardig aan wat SSD's gebruiken, is al jaren in gebruik in USB-sticks, draagbare muziekspelers, mobiele telefoons, geheugenkaarten, enzovoort. Maar de manier waarop gegevens worden beheerd in deze "eenvoudige apparaten" verschilt op veel manieren van de processen die worden uitgevoerd door een SSD en diens controller voor het flash-geheugen.

De interne geheugenchips in SSD's, genaamd NAND-flash, komen sterk overeen met die in andere

apparaten; het verschil is dat een SSD complexe schema's voor gegevensbeheer toepast om gegevens over het geheugen te verdelen. SSD's bevatten tevens een veel groter aandeel aan overcapaciteit (reserve) dat alleen voor de SSD toegankelijk is. Deze en andere processen zijn noodzakelijk om de prestaties en levensduur van de schijf te verlengen – belangrijke voordelen van SSD's. Ze zijn echter verborgen voor de host computer en daarmee voor de gebruiker. Dergelijke verschillen vormen het onderscheid tussen SSD's en de andere op flash gebaseerde opslagmiddelen, en ze vormen de reden voor een aparte aanpak van het wissen.



Op de gebruikelijke manier wissen, levert gevaar op voor SSD's

Vanwege de verschillen in de werking van het flashgeheugen in SSD's, worden aan het wissen daarvan extra eisen gesteld in vergelijking met smartphones, USB-sticks en andere eenvoudiger apparaten. De eisen voor het wissen van SSD's verschillen ook aanzienlijk van die voor het wissen van HDD's, wat al sinds jaren effectief door software wordt gedaan.

Er zijn verschillende benaderingen voor het wissen van gegevens op SSD's, maar elk kent zijn eigen risicofactoren:

Opdrachten voor wissen en formatteren zijn geen geschikte manier van opschonen van een SSD, omdat het mogelijk is dat gegevens op het apparaat achterblijven die vervolgens kunnen worden hersteld door gegevensherstel- of forensische experts.

Fysieke vernietiging maakt een apparaat onbruikbaar en maakt de kans op ROI of het aantonen van duurzame en milieuvriendelijke praktijken onmogelijk. Belangrijker is dat de onjuiste vernietiging van SSD's mogelijkheden biedt aan zeer ervaren tegenstanders om gegevens terug te halen van fragmenten van flash-chips.²

Degaussing heeft succes bij HDD's, maar SSD's gebruiken geïntegreerde circuits voor gegevensopslag, en deze circuits worden elektrisch geprogrammeerd en gewist. Daarom heeft de toepassing van een magnetisch veld geen invloed op de gegevens die op de NAND-flash van een SSD zijn opgeslagen.

Gegevens overschrijven op een SSD met standaarden ontwikkeld voor HDD's, zoals DoD 5220.22-M of HMG, levert mogelijke problemen op met het verwijderen van alle gebruikersgegevens. Dat is het gevolg van de specifieke eigenschappen van een SSD en hoe deze gegevens beheert. Een bewering die door empirische resultaten wordt ondersteund.³

Technieken voor op firmware gebaseerd wissen zoals ATA's Secure Erase zijn niet algemeen betrouwbaar voor SSD's. De reden daarvoor is, dat SSD-fabrikanten geen gestandaardiseerde benadering hebben ontwikkeld voor het wissen van gegevens.⁴

Cryptografisch wissen ruimt een schijf op door aanpassing van de sleutel die gebruikt wordt voor het versleutelen van de gegevens, maar de gegevens staan daarna nog steeds op het apparaat omdat dit gevoelig is voor een onjuiste implementatie van het cryptografische systeem. Ook bij het verifiëren van het wissen kunnen problemen optreden.

Selectief wissen kan in verschillende fasen van een levenscyclus van de SSD nodig zijn om individuele bestanden op een schijf veilig op te ruimen. Maar SSD-controllers zijn geneigd om gegevens naar

nieuwe locaties weg te schrijven, in plaats van “in-place”, zodat het moeilijk wordt om te controleren of alle oudere versies van het bestand eveneens verwijderd zijn.

Externe factoren die het wissen van SSD's compliceren

Naast de interne technische complexiteit zijn er ook externe factoren die degenen die behoefte hebben aan het wissen van SSD's een leverancier laten kiezen die in staat is om effectieve technieken voor het wissen van gegevens toe te passen. Deze factoren omvatten verschillen in de technologie die fabrikanten toepassen, in combinatie met wettelijke en regelgevingseisen.

Gebrek aan standaardisatie door OEM's

De snelle acceptatie van SSD's heeft er voor gezorgd dat een groot aantal original equipment manufacturers (OEM's) van SSD's deze opkomende markt willen aanpakken. Waar zoveel OEM's de markt tegelijk vullen, is sprake van een gebrek aan standaardisatie in de elementen rond de SSD-technologie. Industrie-brede acceptatie van criteria, waaronder de benadering van het wissen van gegevens, komt daar soms achteraan.⁵

De hoeveelheid SSD-modellen, met hun verschillen in hardware en processen, maken de beste benadering voor het beheer van het einde van de levenscyclus nog lastiger. Het is niet mogelijk om er van uit te gaan dat het gedrag van de ene SSD overeenkomt met dat van de volgende. Daarom is de kennis en expertise van een aanbieder van verwijdersoftware zo belangrijk.

De keuze van een aanbieder die gegevens verwijdert met een technologie die gedetailleerde rapporten en een certificaat voor het verwijderen oplevert, is van het grootste belang bij het wereldwijd voldoen aan regels en standaarden.

Toename in de wetgeving voor gegevensbescherming en standaarden

Privacy en bescherming van gegevens staan voortdurend in de aandacht en er bestaat een reeks industrie-specifieke standaarden en regels voor gegevensbescherming. Tegelijkertijd wordt ook nieuwe wetgeving ingevoerd. In 2012 werd in de VS de Consumer Privacy Bill of Rights⁶ van kracht, die een krachtige privacybescherming biedt aan consumenten, inclusief de eis voor het verwijderen van gegevens.

In Europa zijn veranderingen in de gegevensbescherming voorgesteld, inclusief eisen voor het verwijderen van onlinegegevens, het gebruik van auditeerbare procedure, en aanbevelingen voor het gebruik van gecertificeerde tools voor het wissen van gegevens⁷. Overtreders kunnen boetes verwachten tot 2% van hun wereldwijde jaaromzet.

Regels en standaarden kunnen per land en per branche verschillen, maar een gemeenschappelijke eis blijft van kracht: aantoonbaar bewijs van het wissen van gegevens. De keuze van een aanbieder die gegevens verwijdert met een technologie die gedetailleerde rapporten en een certificaat voor het verwijderen oplevert, is van het grootste belang bij het wereldwijd voldoen aan regels en standaarden.



De belangrijkste eisen voor het veilig wissen van SSD's

Bedrijven en organisaties zijn afhankelijk van de processen die geboden worden door professionele bedrijven voor het wissen van gegevens, om hun gegevens te beveiligen. Het niet begrijpen van de uitdagingen die SSD's vormen, resulteert in de toegenomen kans op een inbreuk. Professionele software voor het wissen van gegevens moet aan een aantal belangrijke eisen voldoen om geslaagd wissen van SSD's te garanderen.

Tests en verificatie door derden

Bij het ontwikkelen van een proces voor het wissen van SSD's is het voor een softwareleverancier van het grootste belang dat een onafhankelijk extern bedrijf met forensische expertise en ervaring met gegevensherstel de wisprocessen verifieert en analyseert. Dit is de meest effectieve en onbevooroordeelde manier om de robuustheid van het wisproces te beoordelen. Alleen de aanbieder van een technologie voor het wissen van gegevens die een dergelijke stringente en erkende forensische test heeft ondergaan, kan zeggen dat hij een geslaagde oplossing aanbiedt voor het wissen van SSD's en andere opkomende technologieën.

Bij het ontwikkelen van een proces voor het wissen van SSD's is het voor een softwareleverancier van het grootste belang dat een onafhankelijk extern bedrijf met forensische expertise en ervaring met gegevensherstel de wisprocessen verifieert en analyseert.

Aanbieders van het wissen van SSD's moeten elk beschikbaar validatieschema onderzoeken voor het onafhankelijk valideren van hun oplossing. De Asset Disposal and Information Security Alliance (ADISA)

Geavanceerde software voor het wissen van gegevens moet geautomatiseerde methoden toepassen voor het verwijderen van deze blokkerende beveiligingen en er voor zorgen dat de van belang zijnde methoden voor het wissen in de firmware toegankelijk zijn.

heeft een methodologie ontwikkeld voor het testen van verwijdersoftware voor SSD's⁸. De tests, onder leiding van een expert in gegevensbeveiliging, verifiëren het wissen van een SSD aan de hand van de eisen van een gedefinieerde reeks forensische standaarden.

Om het wisproces te meten aan de hand van de meest geavanceerde tactieken die de branche kent, moeten verwijderprocessen eveneens worden getest met behulp van de expertise van experts van wereldklasse op het gebied van gegevensherstel. Bedrijven die zich bezighouden met gegevensherstel en die beschikken over jaren aan ervaring en op maat gemaakte en intern ontwikkelde tools voor gegevensherstel kunnen de nauwkeurigste processen aanbieden voor het beoordelen van de resultaten.

Verkrijgen van een standaard voor het wissen van SSD's

Verwijdersoftware moet wistechnieken toepassen die speciaal zijn ontwikkeld voor het leveren van de best mogelijke beveiliging. In het ideale geval moet de software een standaard voor het wissen van SSD's omvatten die over de mogelijkheid beschikt om alle specifiek

gedrag van SSD's tegen te gaan, evenals de mogelijkheid om alle beschikbare beveiligingsmaatregelen op een schijf zichtbaar te maken. Uit gepubliceerd onderzoek is reeds gebleken dat het vertrouwen op een specifieke verwijdermethode niet is aan te raden en niet universeel geschikt is voor SSD's⁹.

Deze wisstandaard voor SSD's moet een meerlaags benadering voor het wissen bieden, in staat zijn om schijffouten te detecteren en de sterkst mogelijke verificatie verrichten. De processen die worden uitgevoerd op een SSD moeten elementen omvatten die ontworpen zijn om alle vals positieve meldingen op te lossen die deze schijven kunnen doorgeven bij het melden van een geslaagde verwijdering.

Verwijderen van Freeze lock

Een belangrijk aspect bij het wissen van SSD's is toegang verkrijgen tot de interne wisopdrachten van het apparaat. Het BIOS van de meeste modern computers blokkeert de toegang tot deze opdrachten door de beveiligingsfuncties van de schijf te blokkeren (het Freeze lock). De aanwezigheid van Freeze lock kan een aanzienlijke uitdaging betekenen voor het efficiënt en veilig wissen van SSD's, omdat handmatig ingrijpen en fysieke toegang tot de harde schijf vaak de enige manieren zijn om een Freeze lock te verwijderen.

Omdat SSD's opslaggebieden gebruiken die niet toegankelijk zijn voor software, zijn op firmware gebaseerde wistechnieken noodzakelijk voor een veilig opruimproces. Maar zonder de mogelijkheid tot het geautomatiseerd verwijderen van een Freeze lock, wordt dit proces aanzienlijk moeilijker. Het verkrijgen van fysieke toegang tot de SSD is onpraktisch en inefficiënt in omgevingen waar grote hoeveelheden apparatuur worden verwerkt, wat meer tijd en inspanning vereist voor het uitvoeren van activiteiten, met name bij laptops waar de toegang tot de SSD lastig en tijdrovend is. Het vergroot tevens de kans op fouten en zelfs op schade aan de technologie door onjuiste handelingen.

Geavanceerde software voor het wissen van gegevens moet geautomatiseerde methoden toepassen voor het verwijderen van deze blokkerende beveiligingen en ervoor zorgen dat de belangrijkste methoden voor het wissen in de firmware toegankelijk zijn.

Samenwerking leverancier-OEM

Het huidige gebrek aan standaardisatie rond SSD's geeft aan dat het noodzakelijk is dat aanbieders en OEM's van SSD's samenwerken bij het opzetten van een effectieve kennisbank met betrekking tot de werking

van SSD. Dit soort samenwerking zorgt ervoor dat de beste wismethoden gebruikt worden, zodat de beveiligingsfuncties van de OEM toegankelijk zijn en op de juiste manier worden uitgevoerd.

Een doorlopende samenwerking betekent tevens dat leveranciers voor het wissen van gegevens als derden kunnen functioneren bij het valideren van de interne wisprocessen van een OEM en kunnen garanderen dat ze aan de hoogste beveiligingseisen voldoen.



Samenvatting: Professionele tools omzeilen de barrières voor het wissen van een SSD.

In de toekomst worden SSD's een steeds vaker voorkomend opslagalternatief voor zowel consumenten als bedrijven, wat nog meer invloed heeft op de dynamiek van de verwijderindustrie. Om te voldoen aan robuuste beleiden en praktijken voor gegevensbescherming, moeten IT-beheerders en ITAD's de verschillen kennen tussen de eisen voor het wissen van HDD's en SSD's, zodat ze een effectieve verwijder tool kunnen kiezen, met name naarmate de SSD-technologie zich verder ontwikkelt.

Bij de keuze van een tool voor het wissen van gegevens die SSD's goed kan verwerken, is het van essentieel belang om te kijken naar een tool die is ontwikkeld door een leverancier die de vele haken en ogen kent welke aan de SSD-technologie kleven. Anders kan het resultaat een minder geavanceerde tool of methode zijn,

wat de mogelijkheid biedt voor inbreuk op de gegevens en het verwijderen van de mogelijkheden voor lucratieve mogelijkheden voor wederverkoop.

Professionele verwijdersoftware verwijdert de barrières voor het wissen door blokkerende beveiligingen te omzeilen, fouten op de schijf te detecteren en te melden dat de SSD niet in staat is om de wisselhandelingen effectief uit te voeren, zodat alternatieve procedures ingezet kunnen worden om de risico's te beperken. Het uitgebreide wisrapport van de software ondersteunt ook het voldoen aan de verschillende regels en standaarden en levert informatie over de hardware die noodzakelijk is voor de wederverkoop van de apparatuur. Uiteindelijk levert geavanceerde verwijder-software de gemoedsrust dat gevoelige gegevens niet in de verkeerde handen zullen vallen.

Verwijzingen

- ¹ Zhang, Fang, IHS iSuppli, "Hard Disk Drive Market Revenue Set for Double-Digit Decline This Year," February 4, 2013, <http://www.isuppli.com/Memory-and-Storage/News/Pages/Hard-Disk-Drive-Market-Revenue-Set-for-Double-Digit-Decline-This-Year.aspx>
- ² Swanson, Steven, "Destroying Flash Memory-Based Storage Devices," University of California, San Diego, CA, 2011, <http://cseweb.ucsd.edu/users/swanson/papers/TR-cs2011-0968-Grind.pdf>
- ³ Grupp L., Spada F., Swanson S., Wei M., "Reliably Erasing Data From Flash-based Solid State Drives," 2010
- ⁴ Grupp et. al, 2010
- ⁵ Belkasort, "Why SSD Drives Destroy Court Evidence, and What Can Be Done About It," <http://forensic.belkasoft.com/en/why-ssd-destroy-court-evidence>
- ⁶ Obama Administration, "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy," February 2012, <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>
- ⁷ European Commission, January 2012, http://ec.europa.eu/justice/data-protection/index_en.htm
- ⁸ ADISA Product Claims Testing, <http://www.adisa.org.uk/claimstesting/>
- ⁹ Grupp et. al, 2010

Copyright © 2013 Blancco Oy Ltd. Alle rechten voorbehouden. De informatie in dit document geeft de huidige visie van Blancco Oy Ltd weer op de besproken zaken op het moment van publicatie. In verband met veranderende marktomstandigheden kan Blancco niet garanderen dat enig deel van de informatie na de publicatiedatum accuraat is. Dit Whitepaper dient slechts ter informatie. Blancco biedt in dit document geen garantie, hetzij expliciet of verondersteld.

Het is de verantwoordelijkheid van de gebruiker om te voldoen aan alle toepasselijke auteursrechtenwetgeving. Zonder de rechten onder copyright te beperken, mag niets uit deze uitgave mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand en/of openbaar gemaakt in enige vorm of op enige wijze (elektronisch, mechanisch, door fotokopieën, opnamen of anders) of met enig doel, zonder voorafgaande schriftelijke toestemming van Blancco.



0800 5765 565, info@krollontrack.nl
www.ontrackdatarecovery.nl