# Anlage
# Sicheres Löschen von Datenträgern

Durch die technischen Eigenschaften der verschiedenen Medien prägen sich verschiedene Handlungsalternativen aus. Unterschieden wird zwischen halbleiterbasierten Speichermedien (SSD) und mit magnetischen Medien arbeitenden Festplatten (HDD), sowie Kombinationen (SSHD). Optische, andere magnetische Datenträger und defekte Medien können nur zerstört werden. Bei SSDs / SSHDs muss zwischen verschiedenen Schnittstellen, ATA und NVMe, unterschieden werden.

# 1 Technische Hintergrundinformation

## 1.1 Funktionsweise: Normales Löschen

Beim „**normalen Löschen**“ von Dateien werden lediglich die Verweise auf die Daten im Dateisystemindex, dem Inhaltsverzeichnis der Festplatte, gelöscht und der Bereich zum Überschreiben freigegeben. Dieses Überschreiben findet aber möglicherweise nie statt. Die vermeintlich entsorgten Daten befinden sich auch weiterhin auf der Festplatte und sind u.U. mit einfachen Mitteln erreichbar.

## 1.2 Funktionsweise: (High-Level / Normales) Formatieren

Selbst das „**vollständige Formatieren**“ einer Festplatte oder eines Datenträgers kann unter Umständen Daten nicht vollständig löschen. Bei der „**normalen Formatierung**“, der sogenannten „**High-Level-Formatierung**“, wird lediglich die Dateisystemstruktur neu angelegt; also das komplette Inhaltsverzeichnis gelöscht und durch ein neues ersetzt. Auch hier sind die digitalen Daten physikalisch noch auf dem Datenträger vorhanden und könnten weiterhin ausgelesen werden. Eine „**normale Formatierung**“, z.B. mit Bordmitteln des Betriebssystems, ist als sicheres Löschverfahren somit ungeeignet solange nicht sichergestellt ist, dass der komplette Datenträger überschrieben wurde.

## 1.3 Herausforderung: halbleiterbasierte Speichermedien

Beim „**sicheren Löschen**“ von Daten muss vorangestellt werden, dass dies nur für solche Daten gilt, auf die eine Software als Überschreibprogramm einen Zugriff hat. **Moderne halbleiterbasierte Speichermedien (SSD)** und auch die mit **magnetischen Medien** arbeitenden Festplatten **(HDD)** oder **Kombinationen (SSHD)** verwenden sehr komplizierte Mechanismen, um auftretende Fehler zu beherrschen.

Diese Mechanismen sind im sogenannte Flash Translation Layer (kurz FTL) des Datenträgers implementiert. Dieses Layer koordiniert die Zuordnung zwischen logischem (die Sicht des*r Nutzers*in) und physikalischem Speicher. Hierdurch wird der direkte Zugriff auf eine spezifische Adresse, wie es zum Beispiel bei einer HDD-Festplatte möglich ist, verhindert. Zudem wird jeder einzelne Schreib- und Löschbefehl vom Controller koordiniert. Dadurch wird die SSD zwar schneller und langlebiger, da alle Daten möglichst gleichmäßig verteilt werden, neu geschriebene Daten landen aber nicht zwangsläufig an derselben Stelle, wie die zuvor gelöschten. Durch diesen Umstand versagen die herkömmlichen Löschmethoden mit ihrer Überschreiben-Logik nahezu vollständig bei modernen halbleiterbasierten Speichermedien. Mit speziellen Analyse-Programmen lassen sich die kompletten (gesperrten/geschützten) Speicherbereiche gegebenenfalls auslesen, soweit dies physikalisch noch möglich ist.

## 1.4 Option: Überschreiben von Festplatten mit magnetischem Datenträger (HDD)

Daten auf intakten magnetischen Festplatten (HDD) können mit spezieller Software durch Überschreiben vollständig und nicht wiederherstellbar gelöscht werden. Dabei werden die Daten einmal oder mehrfach mit vorgegebenen Zeichen oder Zufallszahlen überschrieben, was in den meisten Fällen ausreichend ist.

## 1.5 Option: Sicheres Löschen von halbleiterbasierten Speichermedien (SSD, SSHD), Sicheres Löschen von „modernen“ magnetischen Datenträgern (moderne HDD)

Moderne Festplatten – ab dem Jahr 2001 – erlauben die Anwendung der Befehle „ATA-Security Erase" und „ATA-Enhanced Security Erase". Hierbei wird eine herstellerspezifische Routine im Datenträger angestoßen, welche die gesamte Festplatte inklusive defekter Speicherbereiche löschen soll.

Beim „ATA-Security Erase" werden alle Datenbereiche mit Nullen überschrieben. „ATA-Enhanced Security Erase" schreibt vorbestimmte Datenmuster (vom Hersteller festgelegt) in alle Datenbereiche.

Vorsicht: Verschiedene wissenschaftliche Arbeiten[1] haben gezeigt, dass dieses Feature nicht immer auf die richtige Weise implementiert ist, und manchmal werden die Daten nicht einmal gelöscht. Eine Kontrolle auf Erfolg ist also zwingend erforderlich. Trotzdem wird diese Löschmethode bei SSD oder SSHD in Kombination mit einer Überprüfung empfohlen. Einige Hersteller liefern zu ihren SSDs passende Dienstprogramme mit aus, die neben einer Reihe von anderen Tools auch diesen Befehl zum „Reset“ oder „Sicheren Löschen“ der SSD enthalten.

Moderne HDDs unterstützen häufig diese Befehle ebenso und bieten dadurch eine sichere Löschmethode an. Eine Kontrolle auf Erfolg ist auch hier zwingend erforderlich.

Einige SSD-Hersteller bieten eine weitere Option zum Löschen des Laufwerks. Hier gibt es neben der Funktion „ATA-Secure Erase” auch die Funktion „ATA-Sanitize”. Dabei überschreibt die Festplatte nicht nur die Zuordnungstabelle der SSD, sondern löscht auch alle beschriebenen Blöcke. Falls der Datenträger die Funktion „ATA-Sanitize” beherrscht, sollte diese auch benutzt werden.

Alle Datenträger, die gerade eine der o.G. Funktionen ausführen, dürfen während der Laufzeit nicht vom Strom getrennt werden. Üblicherweise kann man diesen Prozess nicht abbrechen.

## 1.6 Option: Defekte Datenträger

Wenn ein Datenträger nicht überschrieben werden soll, oder z.B. wegen eines Defekts nicht überschrieben werden kann, so muss der Datenträger physisch zerstört werden. Das gilt auch für Speichermedien wie CD/DVDs oder USB-Sticks.

## 1.7 Verschlüsselung hilft präventiv

Daten können auch mit Verschlüsselungssoftware und einem nicht leicht erratbaren Schlüssel vor dem Wieder-Auslesen geschützt werden. Aktuelle Tablets und Smartphones verschlüsseln ihre Daten bereits standardmäßig.

# 2 Übersicht der Maßnahmen

1. Sicheres Löschen durch spezifische Befehle des Datenträgers
    a. ATA Halbleiterbasierte Speichermedien (SSD, SSHD)
        i. „ATA-Secure Erase“
        ii. „ATA-Enhanced Secure Erase“
        iii. „ATA-Sanitize“

    b. NVMe Halbleiterbasierte Speichermedien (SSD)
        i. „NVMe-Secure Erase“

    c. ATA Festplatten mit magnetischem Datenträger (HDD)
        i. „ATA-Secure Erase“
        ii. „ATA-Enhanced Secure Erase“

2. Vollständiges Überschreiben des Datenträgers
    a. ATA Festplatten mit magnetischem Datenträger (HDD)
        i. (Mehrfaches) vollständiges Überscheiben des Datenträgers mit Mustern oder Zufallsdaten

3. Vernichten / Zerstören des Datenträgers
    a. Optische Datenträger
    b. Defekte Datenträger
    c. Magnetische Datenträger (z.B. Bänder)

Das „sichere Löschen“ durch spezielle Befehle der Datenträger funktionieren u.U. nicht korrekt. Die Probleme treten häufig bei der Verwendung von

- Firewire-Adapter oder USB-Adapter
- Raid- und SAS-Controller
- Vereinzelt Notebook-BIOSe

auf.

Bei allen Löschversuchen muss der Erfolg kontrolliert werden.

# 3 Werkzeuge: Sicheres Löschen oder Überschreiben von HDD, SSHD, SSDs

Zur einfachen Nutzbarkeit werden drei Werkzeuge vorgestellt.

1. BIOS-Funktionen, einige neuere Mainbords in PCs bieten eine Löschfunktion für Festplatten. Diese sollten Sie bevorzugen. Bitte schauen Sie in die Unterlagen Ihres Gerätes.

2. Windows 10 bietet bereits Bordwerkzeuge zum Löschen von Datenträgern, auf denen sich nicht das Betriebssystem befindet. Allerdings überschreiben diese Programme die Daten nur mit Nullen und sind daher ungeeignet für ein sicheres Löschen. Sie sollten nur verwendet werden, wenn sichere Alternativen nicht greifbar sind.

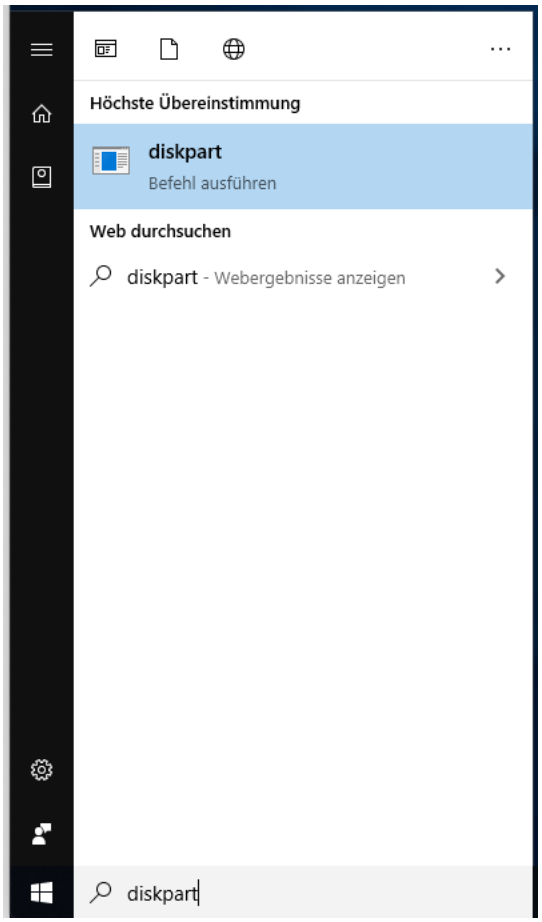
3. Die Hersteller der SSDs bieten eigene Tools zur Verwaltung ihrer Produkte, hier ein paar Links:

    a. **Corsair:**Corsair SSD Toolbox
    b. **Crucial:**Crucial Storage Executive
    c. **Kingston:**SSD Manager
    d. **Kioxia:**SSD-Verwaltungsdienstprogramm
    e. **Intel:**Intel SSD Toolbox
    f. **Samsung:**Samsung Magician
    g. **Sandisk:**SanDisk SSD Dashboard
    h. **Toshiba:**SSD Utility
    i. **WD:**Western Digital SSD Dashboard

    Welche Festplatte(n) Sie haben, erfahren Sie im Gerätemanager unter der Position Laufwerke. Tastenkombination: Win+x, dann im Menü Gerätemanager auswählen und dort Laufwerke.

## 3.1 Bordmittel DiskPart Windows 10

DiskPart ist ein bordeigenes Kommandozeilentool von Windows, das Festplatten mit binären Nullen überschreibt. Dies genügt den Sicherheitsanforderungen, dass mit verschiedenen Mustern mehrfach überschrieben werden soll, nicht. Allerdings ist es ein einfaches und gut erreichbares Mittel, das angewendet werden kann, falls keine andere Option zur Verfügung steht. Systempartitionen von aktuell laufenden Systemen können nicht gelöscht werden.

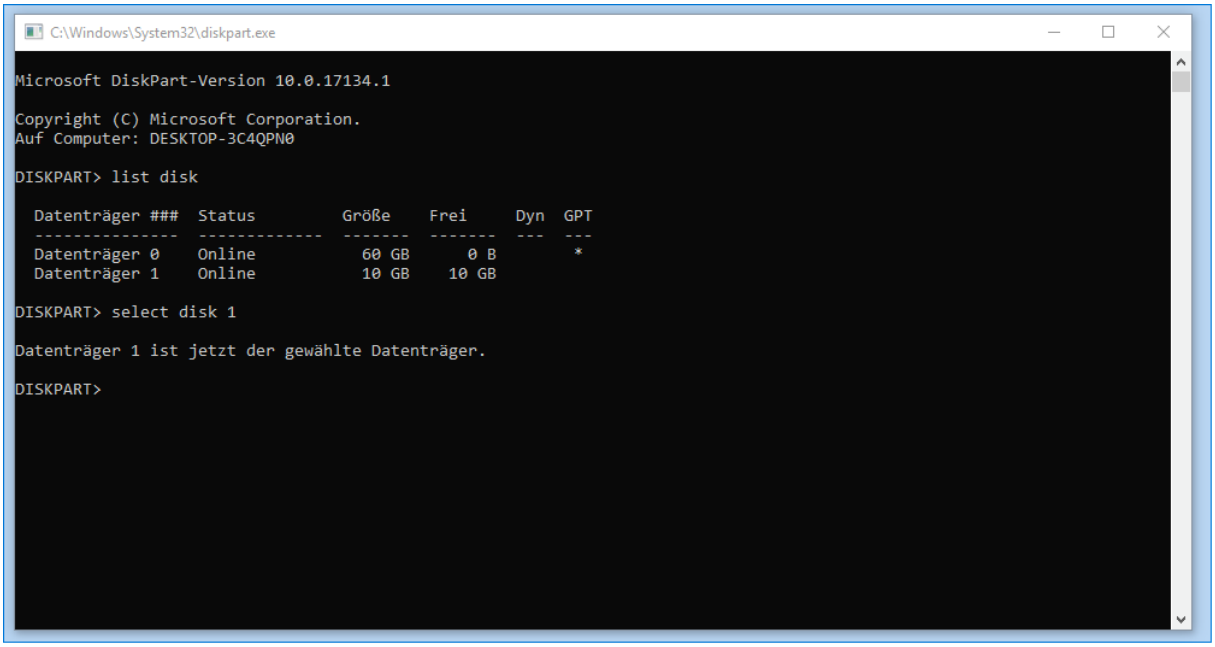



Geben Sie im Suchfeld `diskpart` ein, um das Tool zu starten.

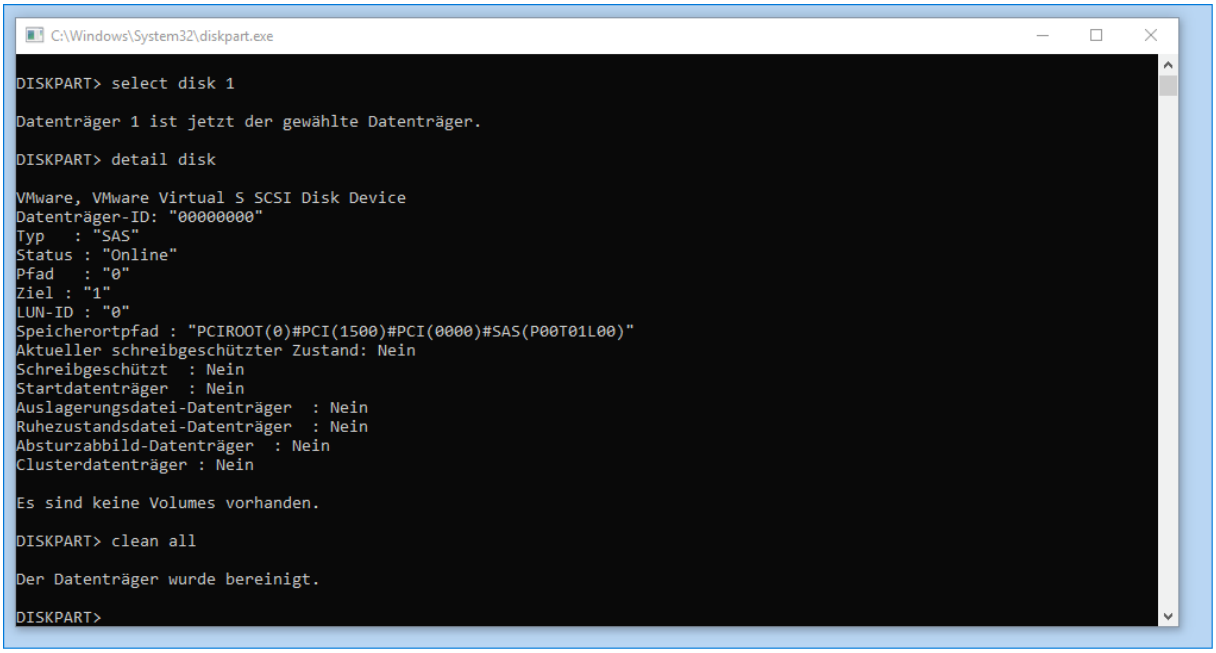

DiskPart muss mit Administratorrechten gestartet werden.

| Befehl | Beschreibung |
|---|---|
| `list disk` | Listet alle im System vorhandenen Datenträger auf. Die Nummer in der Spalte ### müssen Sie sich merken. |
| `select disk <Nummer>` | Hiermit wählen Sie den gewünschten Datenträger für weitere Aktionen. |
| `detail disk` | Prüfen Sie, ob Sie den richtigen Datenträger gewählt haben. Hier sollte der korrekte Hersteller abzulesen sein. |
| `clean all` | Entfernt alle Partitions- oder Volumenformatierungen von dem gewählten Datenträger. Das Schlüsselwort ‚all' gibt an, dass jedes Byte \ jeder Sektor auf dem Datenträger auf mit binären Nullen überschrieben wird. Damit werden alle auf dem Datenträger vorher enthaltenen Daten überschrieben. |

Nach dem Start des Tools kann durch Nutzung der folgenden Befehle die Festplatte überschrieben werden.




(Evtl. Erläuterung zur Auswahl/Eingabe)


C:\Windows\System32\diskpart.exe
DISKPART> select disk 1
Datenträger 1 ist jetzt der gewählte Datenträger.
DISKPART> detail disk
VMware, VMware Virtual S SCSI Disk Device
Datenträger-ID: "00000000"
Typ : "SAS"
Status : "Online"
Pfad : "0"
Ziel : "1"
LUN-ID : "0"
Speicherortpfad : "PCIROOT(0)#PCI(1500)#PCI(0000)#SAS(P00T01L00)"
Aktueller schreibgeschützter Zustand: Nein
Schreibgeschützt : Nein
Startdatenträger : Nein
Auslagerungsdatei-Datenträger : Nein
Ruhezustandsdatei-Datenträger : Nein
Absturzabbild-Datenträger : Nein
Clusterdatenträger : Nein
Es sind keine Volumes vorhanden.
DISKPART> clean all
Der Datenträger wurde bereinigt.
DISKPART>

# 4 Empfehlung: Sicheres Löschen von Smartphones und Tablets

Ob und wie Daten auf Smartphones und Tablets gelöscht werden können, ist je nach Gerät unterschiedlich. Aktuell gibt es kein einheitliches Verfahren oder Standards für ein sicheres Löschen auf Smartphones oder Tablets. Die hier angegeben Maßnahmen sind nur als „Best Effort“ zu betrachten.

Der erste Schritt zum Löschen der Daten vom Smartphone oder Tablet ist (falls möglich) das Entfernen der SD-Karte, im zweiten Schritt setzen Sie das Gerät auf den Werkszustand zurück.

Dazu gehen Sie in den Einstellungen zum Punkt "Sichern & Zurücksetzen“. Auf jüngeren Android-Geräten sollten anschließend keine Daten mehr vorhanden sein: Android setzt ab Version 4.3 regelmäßig einen Trim-Befehl ab, der die Datenreste löscht. Weil unklar ist, wann das passiert, sollten Sie die Geräte noch einige Stunden eingeschaltet am Ladegerät hängen lassen.

Auf Android-Geräten ab Version 6.0 und Smartphones mit iOS und Windows Phone ist der interne Flash-Speicher verschlüsselt. Hier genügt das einmalige Zurücksetzen auf den Werkszustand.

Bei älteren Android-Geräten (vor Version 4.3) können auch nach dem Werks-Reset noch Datenreste zu finden sein. Um diese zu entfernen, schließen Sie das Mobilgerät per USB an den PC. Wird es dabei im Dateimanager als Laufwerk erkannt, schreiben Sie, z.B. mit H2testw (siehe Quellen), den kompletten Speicher mit Zufallsdaten voll und löschen anschließend die erzeugten Testdateien.

Alternativ laden Sie sich nach Reset und neuerlichem Einrichten des Telefons ein Tool wie iShredder oder Secure Wipe aus dem Play Store. Mit diesen können Sie den gesamten freien Speicherplatz löschen.

Anschließend muss das Smartphone erneut zurückgesetzt werden.

# 5 Ultima Ratio: Physikalische Vernichtung

Können Datenträger nicht sicher gelöscht werden, muss eine physikalische Vernichtung stattfinden. Diese Vernichtung erfolgt wie in der Abfallbroschüre der Universität geregelt:

Halbleiterbasierte Speichermedien (SSD, SSHD) sowie Festplatten mit magnetischem Datenträger (HDD) müssen aus dem Gerät ausgebaut werden. Diese werden zusammen mit anderen z.B. optischen oder magnetische Datenträgern (z.B. CDs oder Bänder) beim Zentralen Sonderabfalllager (ZSL) mit dem Hinweis abgegeben, dass sich schützenswerte Daten auf ihnen befindet. Dort werden diese Geräte gesammelt und zentral datenschutzgerecht vernichtet.

Können Datenträger nicht ausgebaut werden, geben sie bitte das komplette Gerät mit Hinweis auf den Sachverhalt ab.

Falls sie selbstständig bei der Vernichtung wirken müssen, beachten Sie bitte folgende Sicherheits-Hinweise: Einige Festplattenhersteller verwenden Glasscheiben als Träger für die datenspeichernden Beschichtungen. CDs bzw. DVDs können spontan und sehr heftig zersplittern. Einfaches Durchbohren der Datenträger reicht nicht, um die von der Universität anvisierte Schutzklasse zu erreichen. Bei SSD-Festplatten oder USB-Sticks müssen Sie die einzelnen Speicherchips beschädigen.

# 6 Referenzen

Testprogramm H2testw
https://www.heise.de/download/product/h2testw-50539/download

BSI: Daten auf Festplatten richtig löschen
https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Daten-sichern-verschluesseln-und-loeschen/Daten-endgueltig-loeschen/daten-endgueltig-loeschen_node.html