



Sicheres Löschen von Daten auf SSDs

Alexander Neumann - RedTeam Pentesting GmbH
alexander.neumann@redteam-pentesting.de
<https://www.redteam-pentesting.de>

8. IT-Forensik Workshop
FH Aachen
23. Mai 2018



Einleitung

Datenträger löschen
Partitionen/Dateien löschen
Lösungsvorschlag
Zusammenfassung

RedTeam Pentesting, Daten & Fakten
Anwendungsfall
Definitionen

RedTeam Pentesting, Daten & Fakten

- ★ Gegründet 2004 in Aachen
- ★ Spezialisierung ausschließlich auf Penetrationstests
- ★ Weltweite Durchführung von Penetrationstests
- ★ Forschung im Bereich der IT-Sicherheit





Einleitung

Datenträger löschen
Partitionen/Dateien löschen
Lösungsvorschlag
Zusammenfassung

RedTeam Pentesting, Daten & Fakten
Anwendungsfall
Definitionen

Was ist ein Penetrationstest?

- ★ Angriff auf Produkt oder Netzwerk
- ★ Ziel: Das zu erreichen, was nicht passieren darf





Daten löschen

- ★ Es fallen sehr sensible Daten an
- ★ Kunden/Projekte sind voneinander getrennt
- ★ Müssen einzeln lösbar sein
- ★ Mit Festplatten: Kein Problem



Daten löschen

- ★ Es fallen sehr sensible Daten an
- ★ Kunden/Projekte sind voneinander getrennt
- ★ Müssen einzeln löscher sein
- ★ Mit Festplatten: Kein Problem
- ★ Nun: Anschaffung neuer Laptops
- ★ Natürlich mit SSDs!
- ★ Daten löschen auf SSDs kann doch nicht so schwer sein...



Einleitung

Datenträger löschen
Partitionen/Dateien löschen
Lösungsvorschlag
Zusammenfassung

RedTeam Pentesting, Daten & Fakten
Anwendungsfall
Definitionen

Sicheres Löschen

Für uns bedeutet (sicheres) Löschen:

- ★ Vorgang ist „unwiederbringlich“
- ★ Auch ich selbst kann die Daten nicht wiederherstellen





Angreifermodell

Starker Angreifer:

- ★ Physischer Zugriff auf das System und die SSD
- ★ Kenntnisse der Elektrotechnik (SSD, Flash-Speicher)
- ★ Passwörter des Benutzers bekannt

Annahme: Angreifer erhält Zugriff auf das System, direkt nachdem Daten gelöscht wurden.



Einleitung
Datenträger löschen
Partitionen/Dateien löschen
Lösungsvorschlag
Zusammenfassung

Festplatten
Löschen von Festplatten
Grundlagen SSDs
Löschen von SSDs

Festplatten

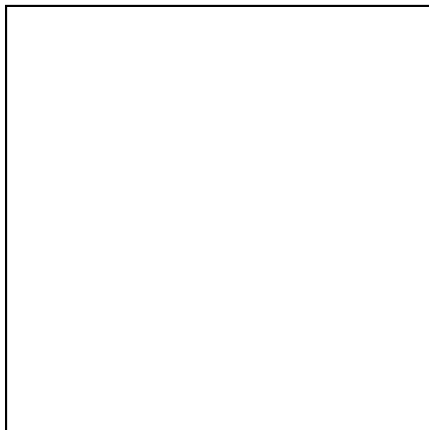




Einführung

- ★ Festplatte
- ★ Blöcke (meist 512 Byte)
- ★ Partitionen (oder LVM)
- ★ Datei A
- ★ Datei B
- ★ Datei C
- ★ Datei D

Festplatte

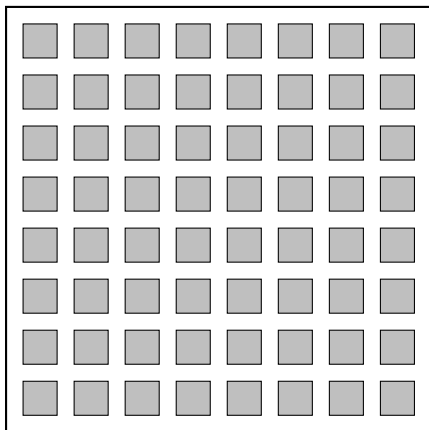




Einführung

- ★ Festplatte
- ★ Blöcke (meist 512 Byte)
- ★ Partitionen (oder LVM)
- ★ Datei A
- ★ Datei B
- ★ Datei C
- ★ Datei D

Festplatte

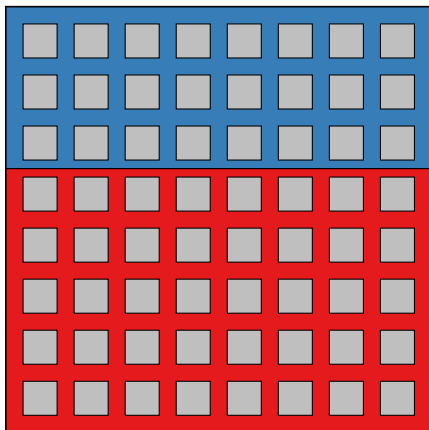




Einführung

- ★ Festplatte
- ★ Blöcke (meist 512 Byte)
- ★ Partitionen (oder LVM)
- ★ Datei A
- ★ Datei B
- ★ Datei C
- ★ Datei D

Festplatte





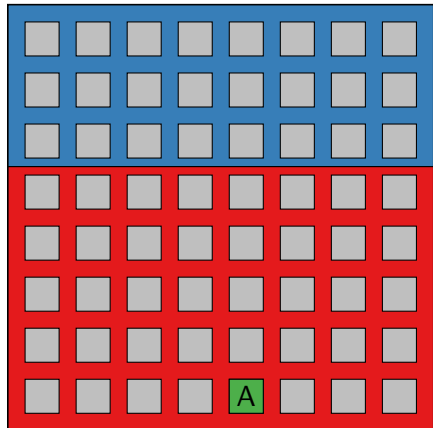
Einleitung
Datenträger löschen
Partitionen/Dateien löschen
Lösungsvorschlag
Zusammenfassung

Festplatten
Löschen von Festplatten
Grundlagen SSDs
Löschen von SSDs

Einführung

- ★ Festplatte
- ★ Blöcke (meist 512 Byte)
- ★ Partitionen (oder LVM)
- ★ Datei A
- ★ Datei B
- ★ Datei C
- ★ Datei D

Festplatte

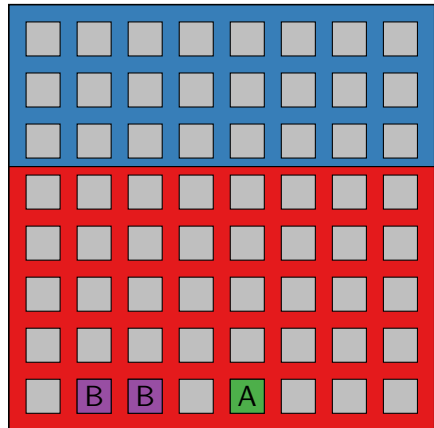




Einführung

- ★ Festplatte
- ★ Blöcke (meist 512 Byte)
- ★ Partitionen (oder LVM)
- ★ Datei A
- ★ Datei B
- ★ Datei C
- ★ Datei D

Festplatte

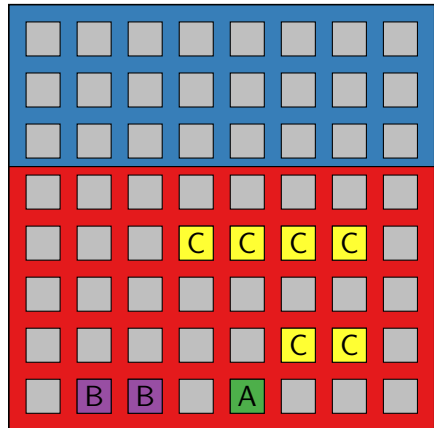




Einführung

- ★ Festplatte
- ★ Blöcke (meist 512 Byte)
- ★ Partitionen (oder LVM)
- ★ Datei A
- ★ Datei B
- ★ Datei C
- ★ Datei D

Festplatte

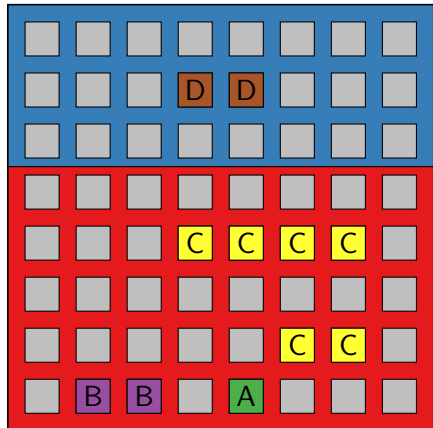




Einführung

- ★ Festplatte
- ★ Blöcke (meist 512 Byte)
- ★ Partitionen (oder LVM)
- ★ Datei A
- ★ Datei B
- ★ Datei C
- ★ Datei D

Festplatte





Löschen von Festplatten

Standardverfahren für Festplatten:

- ★ Überschreiben des gesamten Speichers
- ★ Löschfunktion des Laufwerks (ATA „SECURE ERASE“)
- ★ Physisches Zerstören



Einleitung
Datenträger löschen
Partitionen/Dateien löschen
Lösungsvorschlag
Zusammenfassung

Festplatten
Löschen von Festplatten
Grundlagen SSDs
Löschen von SSDs

SSDs





Einleitung
Datenträger löschen
Partitionen/Dateien löschen
Lösungsvorschlag
Zusammenfassung

Festplatten
Löschen von Festplatten
Grundlagen SSDs
Löschen von SSDs

Besonderheiten SSDs

- ★ Flash-Speicher
- ★ Keine mechanischen Komponenten
- ★ Wahlfreier Zugriff ohne Latenz
- ★ Sehr hohe Datentransferrate
- ★ Over-Provisioning



Einleitung

Datenträger löschen

Partitionen/Dateien löschen

Lösungsvorschlag

Zusammenfassung

Festplatten

Löschen von Festplatten

Grundlagen SSDs

Löschen von SSDs

Löschen einer SSD

These:

SSDs verhalten sich wie Festplatten, da geht das doch genauso!



Löschen einer SSD

BSI

Moderne Festplatten erlauben die Anwendung des ATA-„Secure-Erase“ Befehls. Hierbei wird eine herstellereigene Routine in der Festplatte angestoßen, welche die gesamte Festplatte inklusive defekter Speicherbereiche löschen soll. Bei **SSD** oder SSHD wird diese Löschmethode empfohlen. Die Anwendung von „**Secure Erase**“ sollte mit dem [...] Überschreiben mit Zufallszahlen kombiniert werden.

https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/RichtigLoeschen/richtigloeschen_node.html



Einleitung

Datenträger löschen

Partitionen/Dateien löschen

Lösungsvorschlag

Zusammenfassung

Festplatten

Löschen von Festplatten

Grundlagen SSDs

Löschen von SSDs

Löschen einer SSD

- ★ Physisches Zerstören
- ★ Überschreiben des gesamten Speichers?
- ★ Löschfunktion des Laufwerks (ATA „SECURE ERASE“)?



Einleitung

Datenträger löschen

Partitionen/Dateien löschen

Lösungsvorschlag

Zusammenfassung

Festplatten

Löschen von Festplatten

Grundlagen SSDs

Löschen von SSDs

Löschen einer SSD

- ★ Physisches Zerstören ✓
- ★ Überschreiben des gesamten Speichers?
- ★ Löschfunktion des Laufwerks (ATA „SECURE ERASE“)?



Löschen einer SSD

- ★ Physisches Zerstören ✓
- ★ Überschreiben des gesamten Speichers? ✗
- ★ Löschfunktion des Laufwerks (ATA „SECURE ERASE“)?



ATA „Secure Erase“

Wei et.al. (Usenix FAST, 2011)

„Reliably Erasing Data From Flash-Based Solid State Drives“

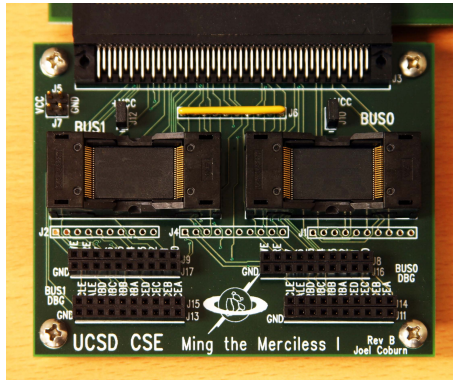
- ★ Direktes Auslesen der Flash-ICs
- ★ Hardware entwickelt, Kosten damals etwa \$1000
- ★ ATA „Secure Erase“ oft fehlerhaft



Einleitung
Datenträger löschen
Partitionen/Dateien löschen
Lösungsvorschlag
Zusammenfassung

Festplatten
Löschen von Festplatten
Grundlagen SSDs
Löschen von SSDs

Wei (2011): Flash-Leser für TSOP-48





Löschen einer SSD

These:

SSDs verhalten sich wie Festplatten, da geht das doch genauso!



Löschen einer SSD

These:

~~SSDs verhalten sich wie Festplatten, da geht das doch genauso!~~



Löschen von Partitionen und Dateien

These:

Aber zumindest das Löschen von Partitionen und Dateien funktioniert doch genauso wie bei Festplatten!



Partitionen löschen auf Festplatten

- ★ Gut abgegrenzt auf der Festplatte
- ★ Enthält meist ein eigenes Dateisystem
- ★ Kann „am Stück“ überschrieben werden
- ★ Das entfernt alle Datenreste (temporäre Dateien, Metadaten)

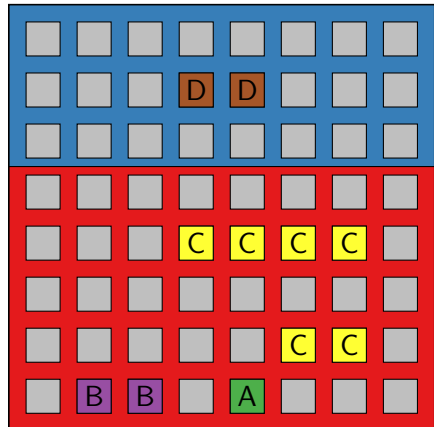
⇒ Gut geeignet, um zu löschende Daten abzulegen



Festplatte: Partition löschen

★ Überschreibe Partition

Festplatte

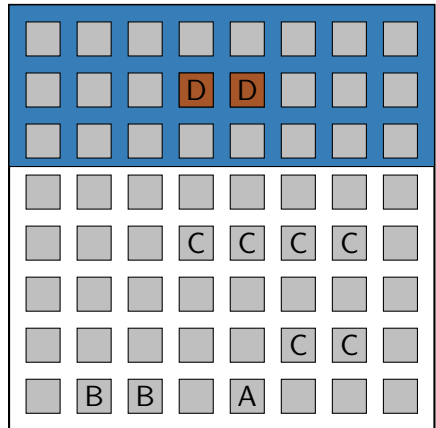




Festplatte: Partition löschen

★ Überschreibe Partition

Festplatte

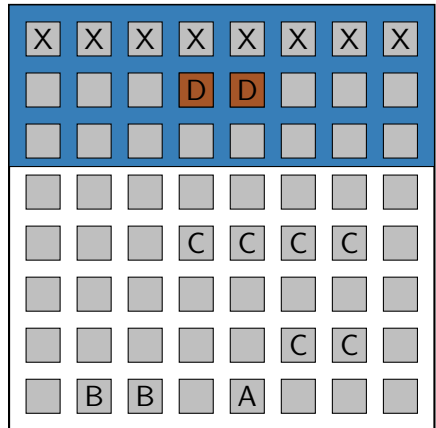




Festplatte: Partition löschen

★ Überschreibe Partition

Festplatte

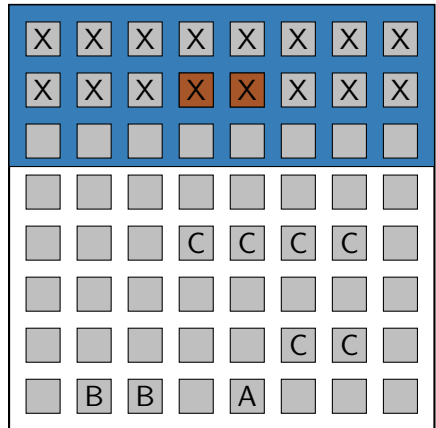




Festplatte: Partition löschen

★ Überschreibe Partition

Festplatte

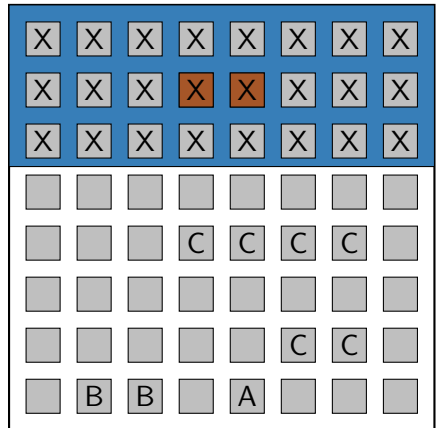




Festplatte: Partition löschen

★ Überschreibe Partition

Festplatte





Einleitung
Datenträger löschen
Partitionen/Dateien löschen
Lösungsvorschlag
Zusammenfassung

Partition löschen auf Festplatten
Dateien löschen auf Festplatten
Besonderheiten von SSDs
Zwischenfazit

Löschen von Dateien auf Festplatten



Löschen von Dateien auf Festplatten

- ★ Dateisysteme bieten kein Interface, um einzelne Blöcke zu finden
 - ★ Temporäre Kopien werden nicht überschrieben, Dateien sind eventuell gar nicht mehr vorhanden
 - ★ Metadaten wie Dateinamen bleiben eventuell erhalten
 - ★ Optimierungen (z.B. Journaling) erschweren das Überschreiben
- ⇒ Freier Speicher der Partition muss überschrieben werden

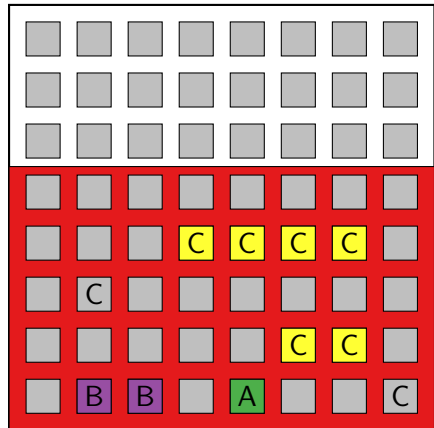


Dateien löschen

Lösche Datei C:

- ★ Blöcke überschreiben
- ★ Datei löschen
- ★ Freie Blöcke überschreiben

Festplatte



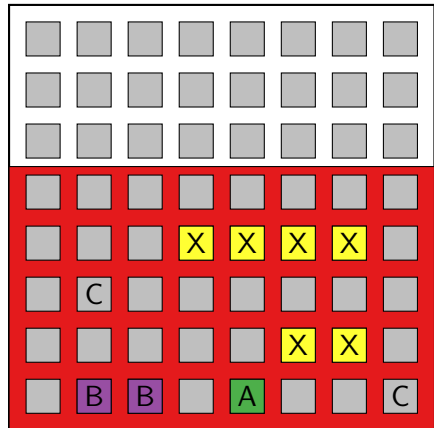


Dateien löschen

Lösche Datei C:

- ★ Blöcke überschreiben
- ★ Datei löschen
- ★ Freie Blöcke überschreiben

Festplatte



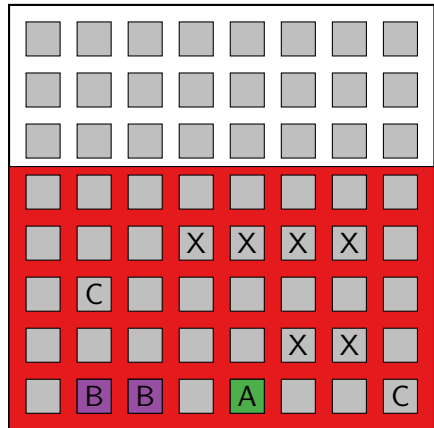


Dateien löschen

Lösche Datei C:

- ★ Blöcke überschreiben
- ★ Datei löschen
- ★ Freie Blöcke überschreiben

Festplatte



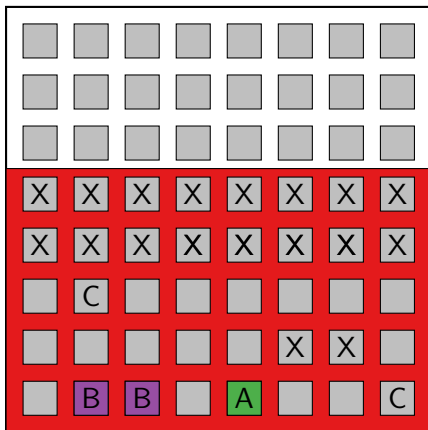


Dateien löschen

Lösche Datei C:

- ★ Blöcke überschreiben
- ★ Datei löschen
- ★ Freie Blöcke überschreiben

Festplatte



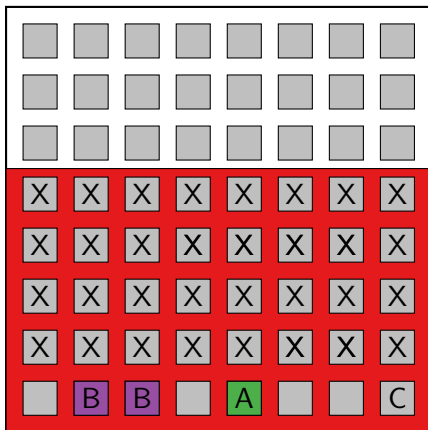


Dateien löschen

Lösche Datei C:

- ★ Blöcke überschreiben
- ★ Datei löschen
- ★ Freie Blöcke überschreiben

Festplatte



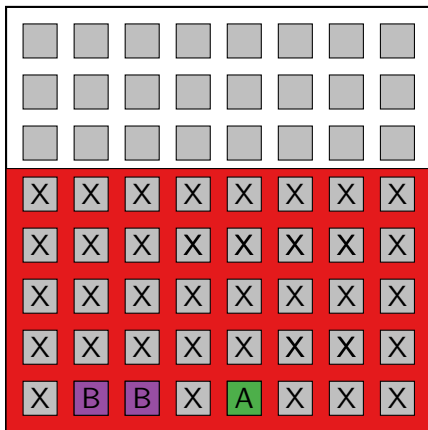


Dateien löschen

Lösche Datei C:

- ★ Blöcke überschreiben
- ★ Datei löschen
- ★ Freie Blöcke überschreiben

Festplatte





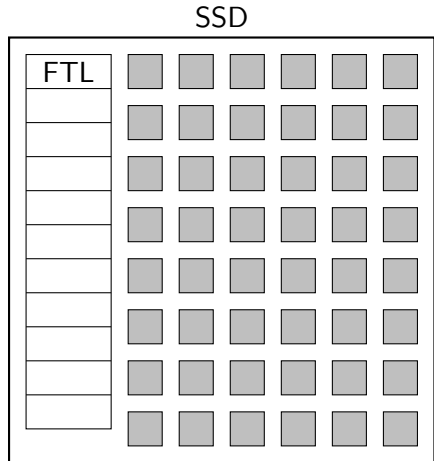
Besonderheiten von SSDs

- ★ Jeder Block kann nur ein mal geschrieben werden
- ★ Blöcke können nur seitenweise geleert werden
- ★ Wear Leveling: Gleichmäßige Nutzung des Flash-Speichers
- ★ Dazu: Flash Translation Layer (FTL)



Flash Translation Layer (FTL)

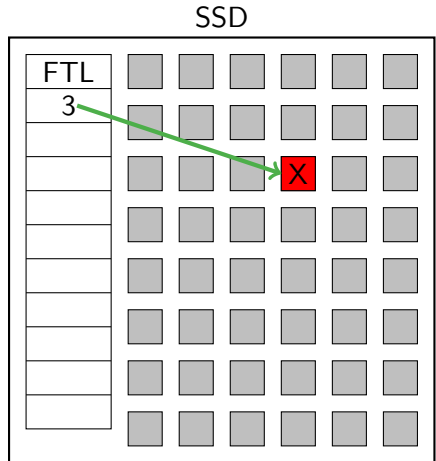
- ★ Schreibe „X“ in Block 3
- ★ Schreibe „Y“ in Block 3
- ★ Schreibe „Z“ in Block 3





Flash Translation Layer (FTL)

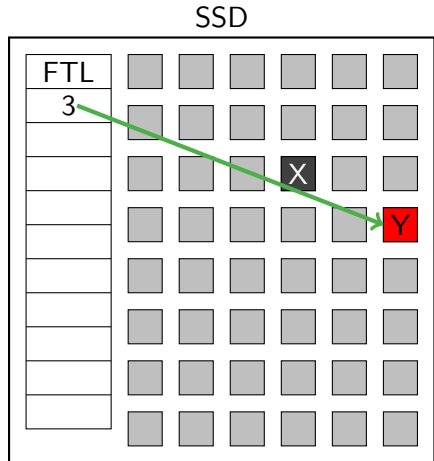
- ★ Schreibe „X“ in Block 3
- ★ Schreibe „Y“ in Block 3
- ★ Schreibe „Z“ in Block 3





Flash Translation Layer (FTL)

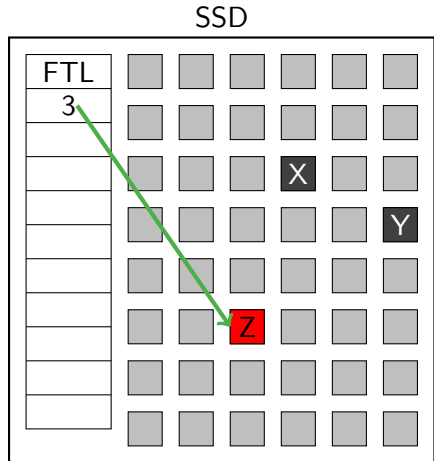
- ★ Schreibe „X“ in Block 3
- ★ Schreibe „Y“ in Block 3
- ★ Schreibe „Z“ in Block 3





Flash Translation Layer (FTL)

- ★ Schreibe „X“ in Block 3
- ★ Schreibe „Y“ in Block 3
- ★ Schreibe „Z“ in Block 3

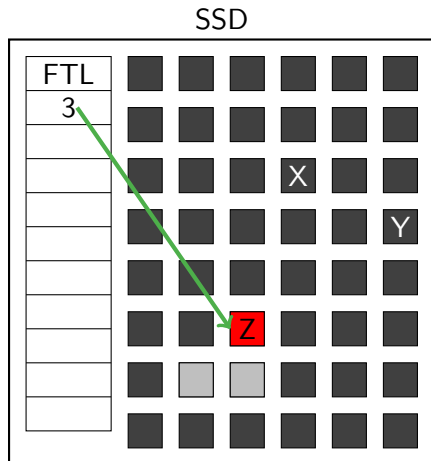




Seitenweises Leeren von Blöcken

Schreibe 4 Blöcke (A, B, C, D):

- ★ Zu wenig leere Blöcke
- ★ Leere ganze Seite
- ★ Schreibe Blöcke

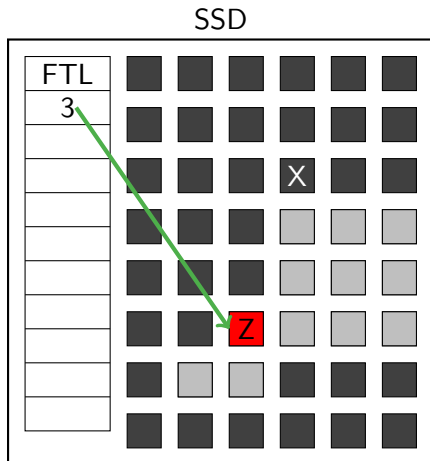




Seitenweises Leeren von Blöcken

Schreibe 4 Blöcke (A, B, C, D):

- ★ Zu wenig leere Blöcke
- ★ Leere ganze Seite
- ★ Schreibe Blöcke

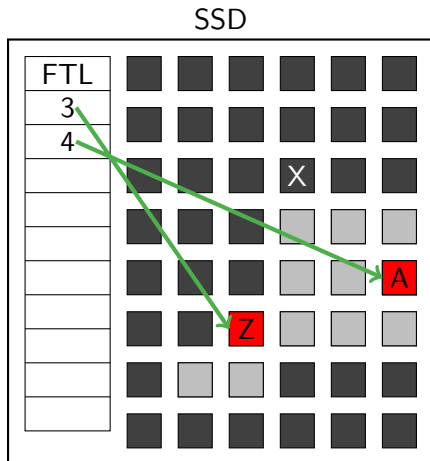




Seitenweises Leeren von Blöcken

Schreibe 4 Blöcke (A, B, C, D):

- ★ Zu wenig leere Blöcke
- ★ Leere ganze Seite
- ★ Schreibe Blöcke

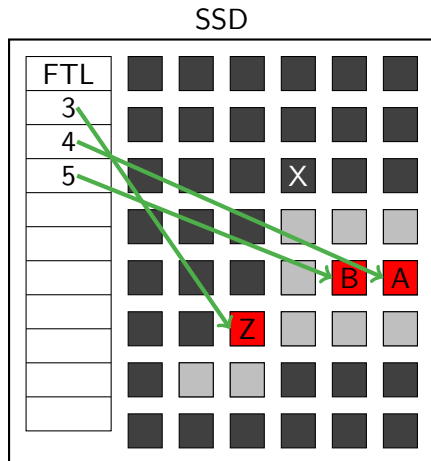




Seitenweises Leeren von Blöcken

Schreibe 4 Blöcke (A, B, C, D):

- ★ Zu wenig leere Blöcke
- ★ Leere ganze Seite
- ★ Schreibe Blöcke

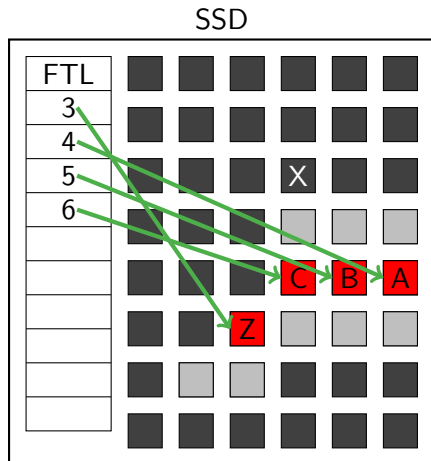




Seitenweises Leeren von Blöcken

Schreibe 4 Blöcke (A, B, C, D):

- ★ Zu wenig leere Blöcke
- ★ Leere ganze Seite
- ★ Schreibe Blöcke

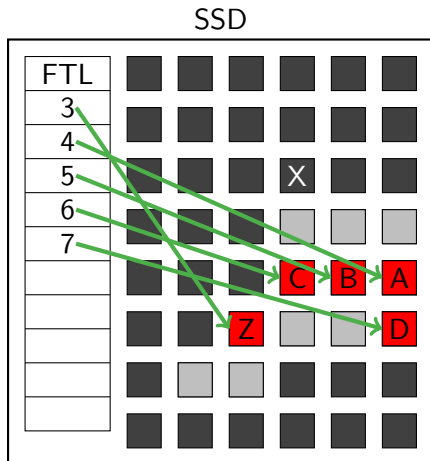




Seitenweises Leeren von Blöcken

Schreibe 4 Blöcke (A, B, C, D):

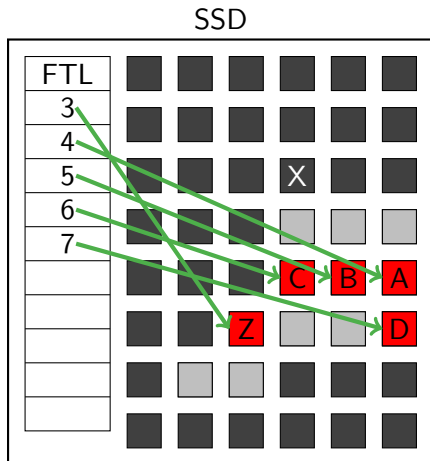
- ★ Zu wenig leere Blöcke
- ★ Leere ganze Seite
- ★ Schreibe Blöcke





Garbage Collection

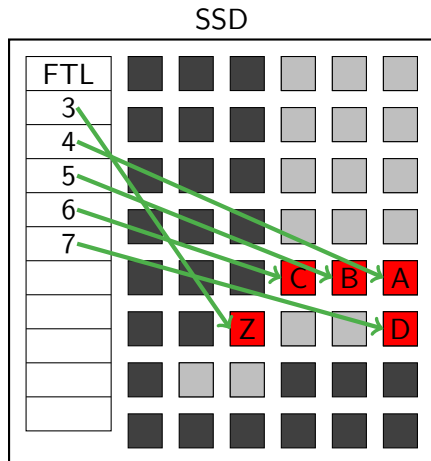
- ★ Leeren von Seiten dauert relativ lange
- ★ SSDs führen GC durch
- ★ Von außen nicht ersichtlic
- ★ Daten werden kopiert





Garbage Collection

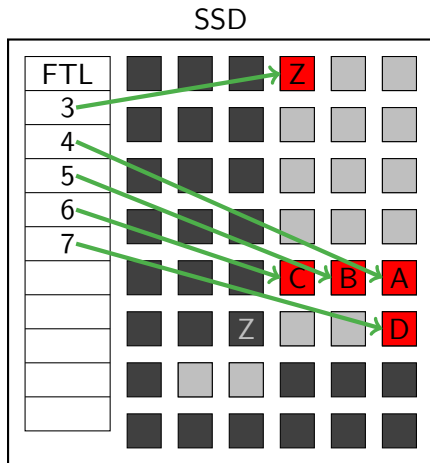
- ★ Leeren von Seiten dauert relativ lange
- ★ SSDs führen GC durch
- ★ Von außen nicht ersichtlic
- ★ Daten werden kopiert





Garbage Collection

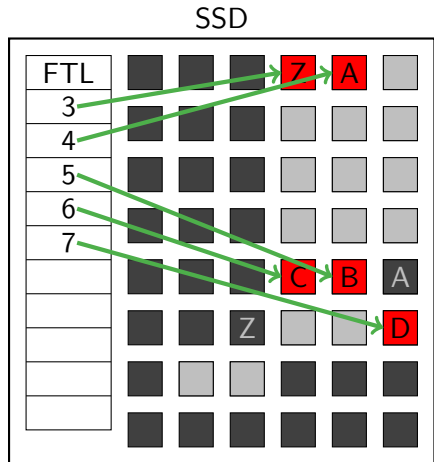
- ★ Leeren von Seiten dauert relativ lange
- ★ SSDs führen GC durch
- ★ Von außen nicht ersichtlic
- ★ Daten werden kopiert





Garbage Collection

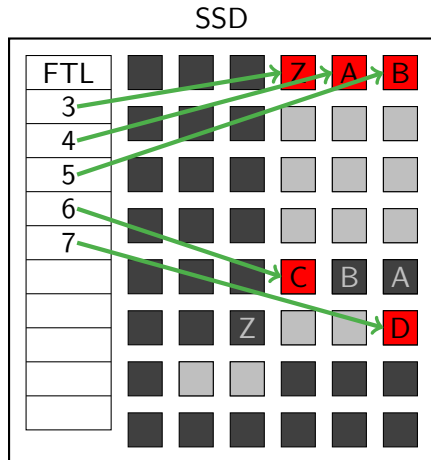
- ★ Leeren von Seiten dauert relativ lange
- ★ SSDs führen GC durch
- ★ Von außen nicht ersichtlich
- ★ Daten werden kopiert





Garbage Collection

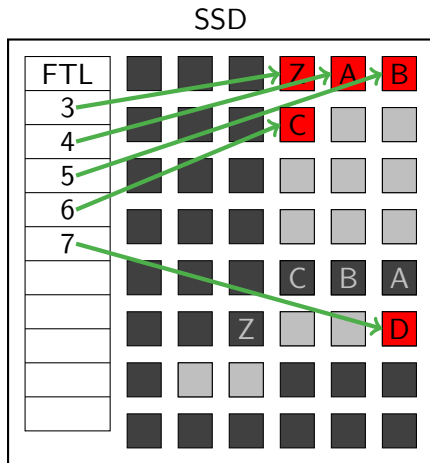
- ★ Leeren von Seiten dauert relativ lange
- ★ SSDs führen GC durch
- ★ Von außen nicht ersichtlic
- ★ Daten werden kopiert





Garbage Collection

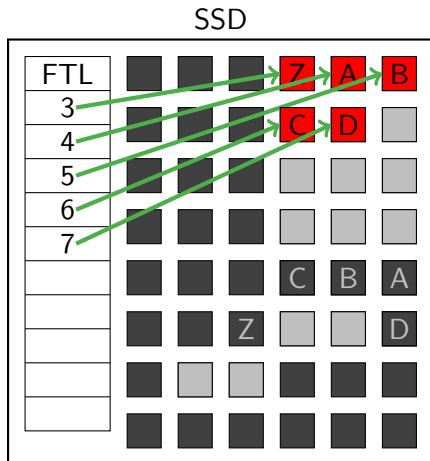
- ★ Leeren von Seiten dauert relativ lange
- ★ SSDs führen GC durch
- ★ Von außen nicht ersichtlic
- ★ Daten werden kopiert





Garbage Collection

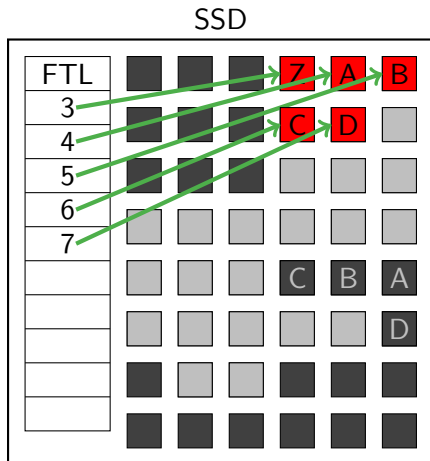
- ★ Leeren von Seiten dauert relativ lange
- ★ SSDs führen GC durch
- ★ Von außen nicht ersichtlich
- ★ Daten werden kopiert





Garbage Collection

- ★ Leeren von Seiten dauert relativ lange
- ★ SSDs führen GC durch
- ★ Von außen nicht ersichtlich
- ★ Daten werden kopiert





Folgerungen für SSDs

- ★ Überschreiben von Daten funktioniert nicht!
 - ★ SSDs erzeugen Kopien von Daten
 - ★ Zusätzlich: Over-Provisioning
- ⇒ Kein unwiederbringliches Löschen!



Realitätsabgleich

Wie realistisch ist es, die Daten aus dem Flash direkt auszulesen?



Einleitung
Datenträger löschen
Partitionen/Dateien löschen
Lösungsvorschlag
Zusammenfassung

Partition löschen auf Festplatten
Dateien löschen auf Festplatten
Besonderheiten von SSDs
Zwischenfazit

AliExpress.com : Buy | x

https://www.aliexpress.com/store/product/NAND-ProMan-Professional-programmer-NAND-NOR-TSOP48-FLASH-programmer-TL866-PLUS-programmer-high-p

Buyer Protection Help Save big on our app! Ship to Germany / USD Go to Global Site (English)

AliExpress I'm shopping for... All Categories Search Cart 0 Wish List Sign In Join My AliExpress

Store: HSEC Technology Co., Ltd. Open: 3 year(s) Top-rated Seller 4242 Positive feedback 99.2% Follow

Store Home Products Sale Items Top Selling New Arrivals Feedback Contact Details

Home > Store Home > Products > Programmer

NAND ProMan Professional programmer (TL866 PLUS programmer)

NAND ProMan Professional nand flash programmer/NAND NOR TSOP48 FLASH programmer TL866 PLUS programmer /high programming speed

★★★★★ 4.9 (57 votes) | 77 orders

Price: ~~US \$135.00~~ / piece
Discount Price: **US \$128.25** / piece **5% off** (2 days left)
Find more deals on the app | Bulk Price >

Shipping: **Free Shipping to Germany via AliExpress Standard Shipping**
Estimated Delivery Time: 21-47 days

Quantity: piece (11 pieces available)

Total Price: **US \$128.25**

Buy Now Add to Cart

Add to Wish List (245 Adds)

Recently Viewed

- 1: Automatically identify the IC Clip
- 2: Programming speed Very fast
- 3: Support 1.8-3.3V Clip
- 4: Super star NAND FLASH PROGRAMMER!
- 5: No need to install Drive and software
- 6: support Windows XP, WIN7, WIN8, WIN8.1 and WIN 10
- 7: USB 2.0 cable



Einleitung
Datenträger löschen
Partitionen/Dateien löschen
Lösungsvorschlag
Zusammenfassung

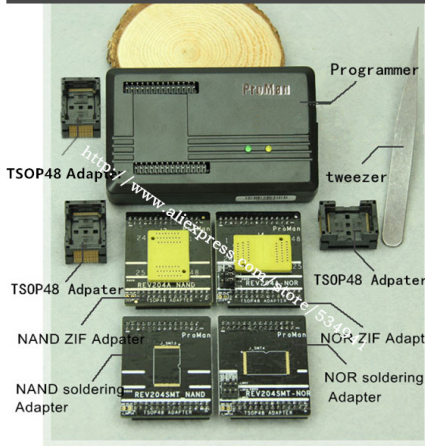
Partition löschen auf Festplatten
Dateien löschen auf Festplatten
Besonderheiten von SSDs
Zwischenfazit

Nand Flash PROGRAMMER





NAND ProMan Professional programmer (TL866 PLUS programmer)



- 1: Automatically identify the IC Clip
- 2 : Programming speed Very fast
- 3: Support 1.8-3.3V Clip
- 4: Super star NAND FLASH PROGRAMMER
- 5: No need to install Drive and software
- 6: support Windows XP, WIN7, WIN8, WIN8.1 and WIN 10
7. USB 2.0 cable



The screenshot shows a software interface for erasing and programming a NAND chip. The interface is divided into several sections, each highlighted with a red box and a number:

- (1)** **<Select Programmer>**: A dropdown menu shows "[#0]Program" and a "Scan" button.
- (2)** **<Bad Block Operations>**: Includes "List BBLK", "BBLK Flag", and checkboxes for "K" and "K".
- (3)** **<Erase and Program>**: Includes "File Name" (programmer/welcome.jpg), "Start Addr (hex)" (0x0), and checkboxes for "Write Spare", "Non-Empty", "Auto Verify", and "Save Difference". Buttons for "Erase Chip", "Program", and "Verify" are present.
- (4)** **<Read>**: Includes "File Name", "Start Addr (hex)" (0x0), "End Addr (hex)" (0x7fffffff), and buttons for "Read" and "Verify After Read".
- (5)** **Process**: A progress bar with 10 blue segments and a "Stop" button.
- (6)** **<Log and Status>**: Includes "Clear Log", "Programmer Info", and "警告CN". A checked "Auto Clear Log" checkbox is visible. The log text shows: "NAND ID: 0xecf10095_0x40ecec f1", "Manufacturer: Samsung", ">>Auto detected successfully.", ">>The parameters are as below:", "*Page data area size2048 bytes.", "*Page spare area size64 bytes.", "*Each block has 64 pages", "*The chip has 1 chip-select signals.", "*There are 1024 blocks each chip-select.", "*Total 1024 blocks each chip.", "*Total memory size 128 Mbytes", "*Range 0x0 - 0x7ffffff", "*Memory type: SLC NAND", "Total 1024 blocks, 1015 good blocks.", "Erase all good blocks successfully."



Einleitung
Datenträger löschen
Partitionen/Dateien löschen
Lösungsvorschlag
Zusammenfassung

Partition löschen auf Festplatten
Dateien löschen auf Festplatten
Besonderheiten von SSDs
Zwischenfazit


0.8MM BGA63 IC prog... x

https://www.aliexpress.com/item/0-8MM-BGA63-IC-programmer-adapter-BGA63-to-DIP48-IC-Test-Socket-9X-11mm-for-NAND/32673564825.html?spm=2114.01

AliExpress™ I'm shopping for... All Categories Q Cart 0 Wish List Sign In Join My AliExpress

Store: HSEC Technology Co., Ltd. Top-rated Seller 4242 99.2% Positive feedback Follow

Back to search results Home > All Categories > Electronic Components & Supplies > Electronics Stocks



0.8MM BGA63 IC programmer adapter/BGA63 to DIP48 IC Test Socket 9X 11mm/
NAND proman / TL866 PLUS + 10.5X13.5MM Matrix

★★★★★ 5.0 (13 votes) | 16 orders

Price: US \$95.00 / piece
Discount Price: **US \$90.25** / piece **5% off** **2 days left**
Find more deals on the app Bulk Price

Shipping: **Free Shipping to Germany via AliExpress Standard Shipping**
Estimated Delivery Time: 21-47 days

Quantity: - 1 + piece (85 pieces available)

Total Price: **US \$90.25**

Buy Now Add to Cart

Add to Wish List (41 Adds)

Return Policy: Returns accepted if product not as described, buyer pays return shipping fee and keep the product & agree refund with seller. View details

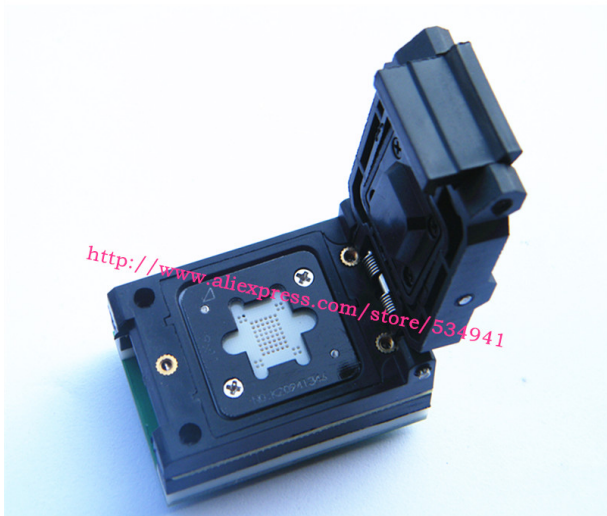
Recently Viewed

BGA63 Programmer Adapter
Pich: 0.8MM



Einleitung
Datenträger löschen
Partitionen/Dateien löschen
Lösungsvorschlag
Zusammenfassung

Partition löschen auf Festplatten
Dateien löschen auf Festplatten
Besonderheiten von SSDs
Zwischenfazit





SSD Datenrettung

Was ist SSD? Datenverlust Ursachen Kundenstimmen Verschlüsselte SSD Platten 0800 10 12 13 14

SSD-Daten retten von allen Herstellern und Modellen

Die Datenrettungs-Experten von Kroll Ontrack retten Daten nicht nur bei SSD-Ausfällen, sondern meistern auch die technischen Herausforderungen, die speziell mit der SSD- und Flash-Technologie zusammenhängen.

Intel®	PatriotMemory®	STEC®
SanDisk®	Samsung®	PNY Technologies®
Western Digital®	Micron®	Crucial®
OCZ® Technology	Kingston Technology®	Transcend®
Toshiba®	Seagate®	Und viele mehr

Die enge Zusammenarbeit mit SSD-Herstellern und unser weltweit tätiges Forschungs- und Entwicklungsteam ermöglicht es Kroll Ontrack einzigartige Datenrettungs-Lösungen von SSD-Platten für Unternehmen und Privatkunden bereitzustellen.

Falls Sie Ihren SSD Hersteller hier nicht entdecken, wenden Sie sich bitte direkt an unsere Mitarbeiter.



Löschen von Partitionen und Dateien

These:

Aber zumindest das Löschen von Partitionen und Dateien funktioniert genauso wie bei Festplatten!



Löschen von Partitionen und Dateien

These:

~~Aber zumindest das Löschen von Partitionen und Dateien funktioniert genauso wie bei Festplatten!~~



Vorteile/Nachteile von SSDs

These:

SSDs sind unsicherer als Festplatten?



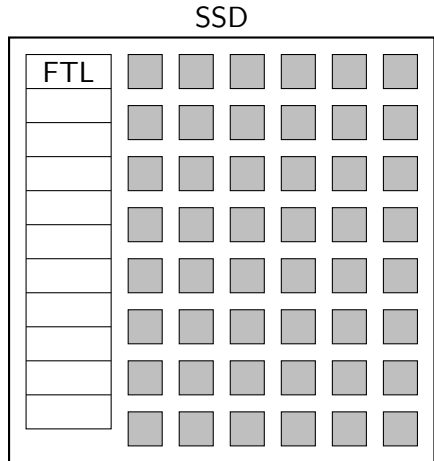
TRIM/DISCARD

- ★ Betriebssystem teilt SSD mit: Block wird nicht mehr benötigt
- ★ Daten können direkt danach nicht mehr gelesen werden
- ★ Aktuelle SSDs implementieren „Read Zero After Trim“ (RZAT)
- ★ Aber: Immer noch gespeichert
- ★ Direktes Auslesen des Flash-Speichers weiterhin möglich
- ★ SSD ist „Black-Box“, keine Kontrolle



TRIM/DISCARD

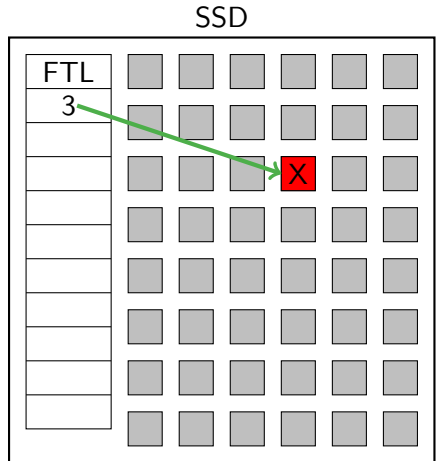
- ★ Schreibe „X“ in Block 3
- ★ Block 3 wird nicht mehr benötigt (TRIM)
- ★ SSD liefert nur Nullen zurück (RZAT)





TRIM/DISCARD

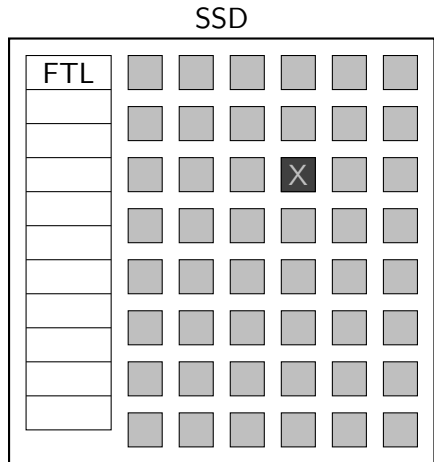
- ★ Schreibe „X“ in Block 3
- ★ Block 3 wird nicht mehr benötigt (TRIM)
- ★ SSD liefert nur Nullen zurück (RZAT)





TRIM/DISCARD

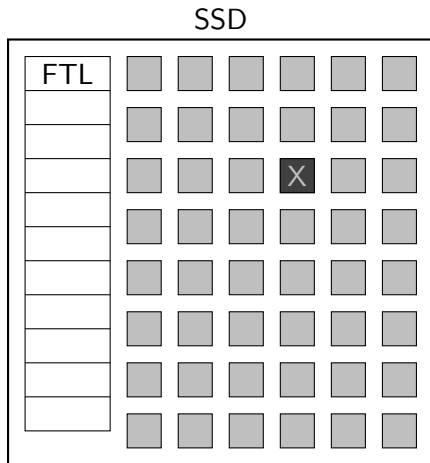
- ★ Schreibe „X“ in Block 3
- ★ Block 3 wird nicht mehr benötigt (TRIM)
- ★ SSD liefert nur Nullen zurück (RZAT)





TRIM/DISCARD

- ★ Schreibe „X“ in Block 3
- ★ Block 3 wird nicht mehr benötigt (TRIM)
- ★ SSD liefert nur Nullen zurück (RZAT)





Vorteil von SSDs mit TRIM/DISCARD

- ★ Gelöschte Dateien zu rekonstruieren ist aufwendiger
- ★ Betrifft auch temporäre Dateien
- ★ Selbst Malware kann gelöschte Dateien nicht lesen



SSDs

These:

SSDs sind unsicherer als Festplatten?



SSDs

These:

~~SSDs sind unsicherer als Festplatten?~~



Zwischenfazit

- ★ SSDs sind sicherheitstechnisch unausgewogen
- ★ Für unseren Anwendungsfall insgesamt schlechter
- ★ Lösung: Daten verschlüsseln?



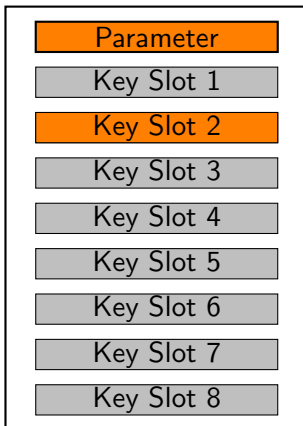
Linux Unified Key Setup (LUKS)

- ★ Header am Anfang der Partition gespeichert
- ★ Bis zu acht Passwörter möglich
- ★ Passwortänderung möglich



Linux Unified Key Setup (LUKS)

LUKS Header

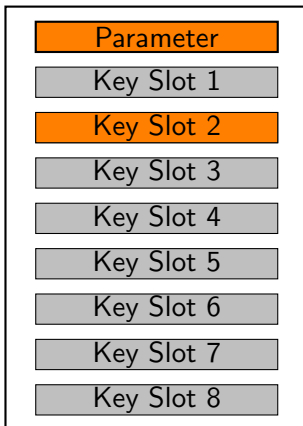




Linux Unified Key Setup (LUKS)

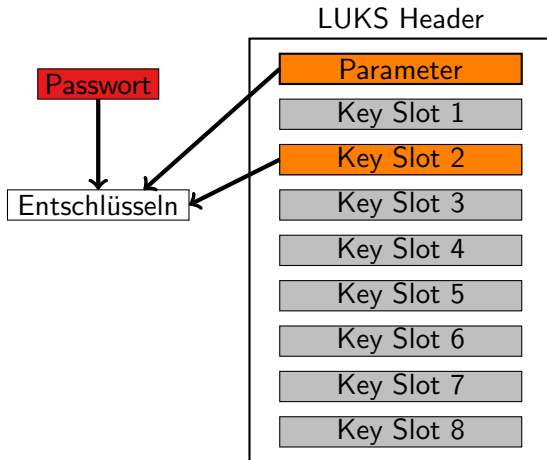
Passwort

LUKS Header



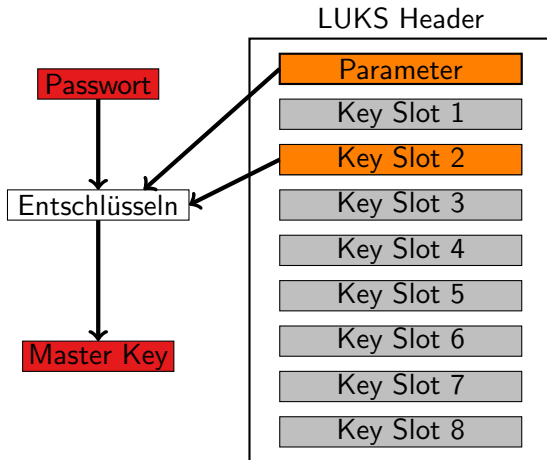


Linux Unified Key Setup (LUKS)





Linux Unified Key Setup (LUKS)





Einleitung
Datenträger löschen
Partitionen/Dateien löschen
Lösungsvorschlag
Zusammenfassung

LUKS
TPM
Implementierung

Linux Unified Key Setup (LUKS)

★ Passwort oder Header gelöscht → Daten gelöscht



Linux Unified Key Setup (LUKS)

- ★ Passwort oder Header gelöscht → Daten gelöscht
- ★ Problem: Header kann auf SSDs nicht gelöscht werden
- ★ Idee: Passwort oder Header woanders speichern?



Trusted Computing Platform (TPM)

- ★ Fast alle Laptops (und viele andere PCs) haben einen TPM-Chip eingebaut
- ★ Hat ein wenig Speicher für Schlüssel (NVRAM)
- ★ Kann sicher gelöscht/überschrieben werden
- ★ Zugriffsschutz per Passwort
- ★ Idee: Speichern eines (Teil-)Passworts im TPM-Chip

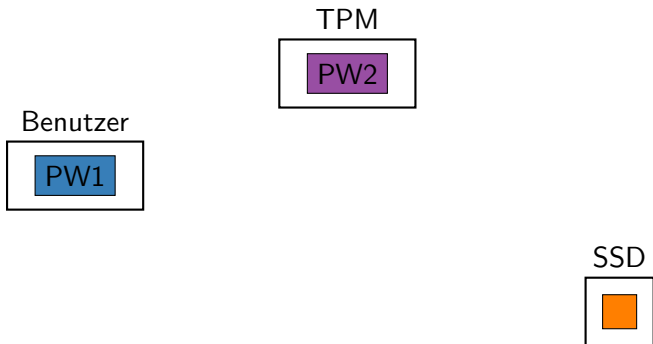


Lösung sicheres Löschen auf SSDs

- ★ Passwort ist zusammengesetzt:
 - ★ Passwort des Benutzers (PW1)
 - ★ Zufällig gewähltes Passwort (PW2)
- ★ PW2 wird im TPM-Chip gespeichert
- ★ Bei der Eingabe des Benutzerpassworts automatisch angehängt
- ★ Benutzer bekommt PW2 nicht angezeigt
- ★ Erweiterung zu cryptsetup (Linux)

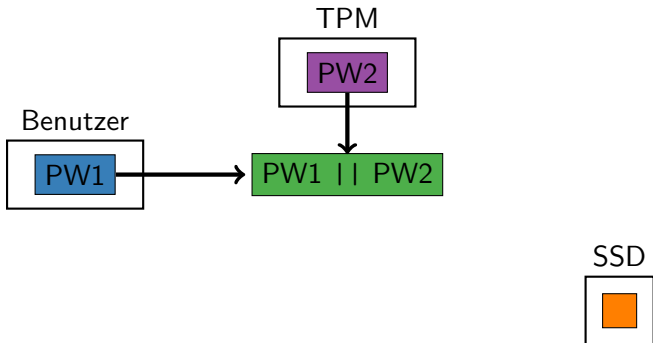


Lösung sicheres Löschen auf SSDs



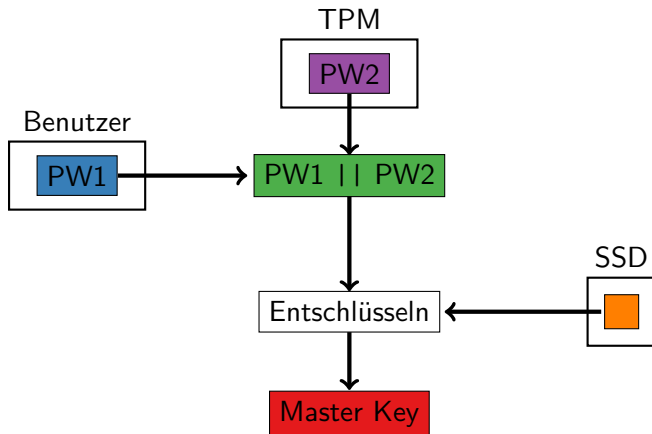


Lösung sicheres Löschen auf SSDs





Lösung sicheres Löschen auf SSDs





Fazit

Fazit:

SSDs sind keine Festplatten!



Fazit

- ★ Große Unterschiede
- ★ Unwiederbringliches Löschen auf SSDs ist nicht möglich
- ★ Lösung vorgestellt: Verschlüsselung mit Teilpasswort im TPM-Chip
- ★ Integration in cryptsetup (Linux) fertig
- ★ Mit dieser Lösung: SSDs insgesamt besser



Ausblick

- ★ Halbleiterbasierte Speichermedien wie SSDs werden zunehmend eingesetzt
- ★ Teilweise auch als Hybridprodukte („SSHD“)
- ★ Festplatten werden ein ähnliches Problem bekommen
- ★ „Shingled Magnetic Recording“ (SMR)



Zeit für Fragen und Diskussionen

Vielen Dank für Ihre
Aufmerksamkeit

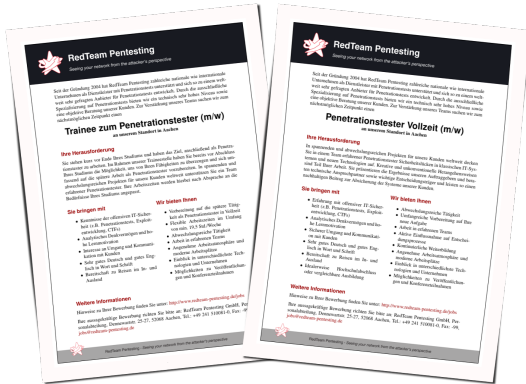
<https://github.com/libnvcrypt/libnvcrypt>
<https://www.redteam-pentesting.de/publications>
Twitter: @RedTeamPT



Datenträger löschen
Partitionen/Dateien löschen
Lösungsvorschlag
Zusammenfassung

Fazit
Ausblick
Fragen

Wir stellen ein!



<https://github.com/libnvcrypt/libnvcrypt>
<https://www.redteam-pentesting.de/publications>
Twitter: @RedTeamPT