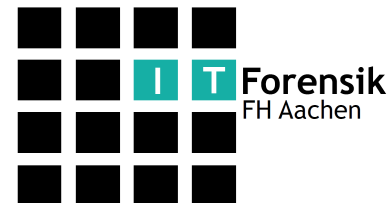


Sicheres Löschen von Mobiltelefonen

Hans Höfken

Lehrgebiet Datennetze, IT-Sicherheit
und IT-Forensik




- Sicheres Löschen, warum?
- Speichertypen im Mobiltelefon
- Speicherarten
- Speicherorte im Mobiltelefon
- Wie kann man Telefone löschen
- Untersuchung und deren Ergebnisse
- Die eigene Android App *SecureErase*


- Smartphone wird für viele tägliche Aktionen eingesetzt
 - Email
 - Termine
 - Dokumente lesen
 - Surfen
 - Navigieren
 - Spielen/Freizeit
 - SMS
 - Verbindung zum Firmennetz
 - ach ja, *telefonieren*



- Korrespondenz
 - Freunde, Bekannte, Kollegen, Bilder, Dokumente ...
- Personen, (private) Treffen, Arbeitsthemen, Orte
- Bücher, private/geschäftliche Dokumente
- Interessen, Filme, Bilder
- Orte, Ziele, Aufenthalte
 - Bluetooth: z.B. in welchem Auto habe ich gesessen
- Freizeitinteressen
- Firmenverbindung, Passworte, IP Adressen
- Telefonbuch, Kontakte

- Typen von Speicherbausteinen (**NAND/NOR**)
 - NAND - Vorteile
 - Hohe Speicherkapazität und sehr geringer Preis pro Megabyte
 - Hohe Schreib- und Lesegeschwindigkeiten bei großen Datenmengen
 - Niedrigere Leistungsaufnahme während der Programmierung
 - Kostengünstige Ankoppelung an Controllersysteme
 - NAND – Nachteile
 - Verglichen mit *NOR-Speichern* ist ein nicht unerheblicher Softwareaufwand erforderlich, um NAND-Speicher korrekt anzusteuern
 - Aufgrund der verwendeten Zugriffsart können NAND-Speicher nicht direkt als Programmspeicher für Mikrocontroller eingesetzt werden
 - 100.000 bis 1.000.000 Schreib-Lösch-Zyklen bei *SLC*, danach ist der Speicher nicht mehr nutzbar.
 - 3.000 bis 10.000 Schreib-Lösch-Zyklen bei *MLC*, danach ist der Speicher nicht mehr nutzbar.

 *SLC*
single-level cell

 *MLC*
multi-level cell

- Typen von Speicherbausteinen (NAND/**NOR**)
 - NOR – Vorteile
 - linear adressierbarer Speicher, ermöglicht Ausführung von Code
 - hohe Schreibgeschwindigkeit bei kleinen Datenmengen
 - problemlose Ankopplung an Controllersysteme aufgrund des SRAM-ähnlichen Bussystems
 - NOR – Nachteile
 - relativ hohe Leistungsaufnahme
 - langsam beim Schreiben und Löschen großer Datenmengen
 - nur für relativ kleine Speicherkapazitäten erhältlich



SRAM
static RAM

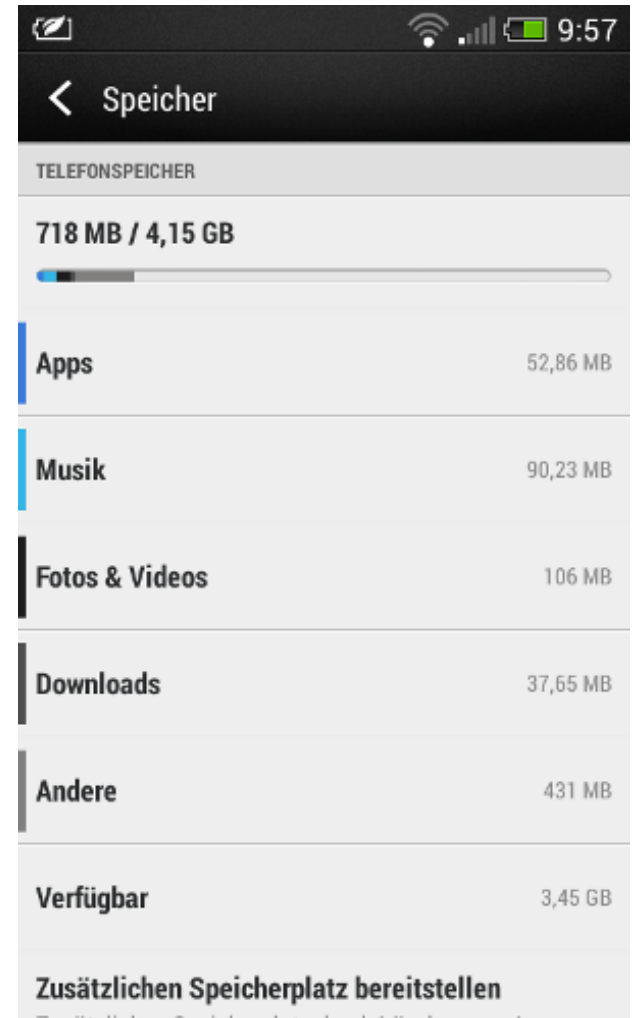
- Kombination aus Verfahren und Mechanismen um die Lebensdauer von Flash-Speicher zu verlängern
 - Statisches Verfahren
 - neue Daten werden auf jeweils anderen freigegebenen Blöcke geschrieben
 - Vorgang ist transparent und benötigt keine Software oder Treiber
 - LRU Mechanismus
 - am wenigsten verwendet Blöcke werden als nächstes beschrieben
- Statisches Verfahren + LRU sorgen für gleichmäßige Abnutzung des Flash-Speichers



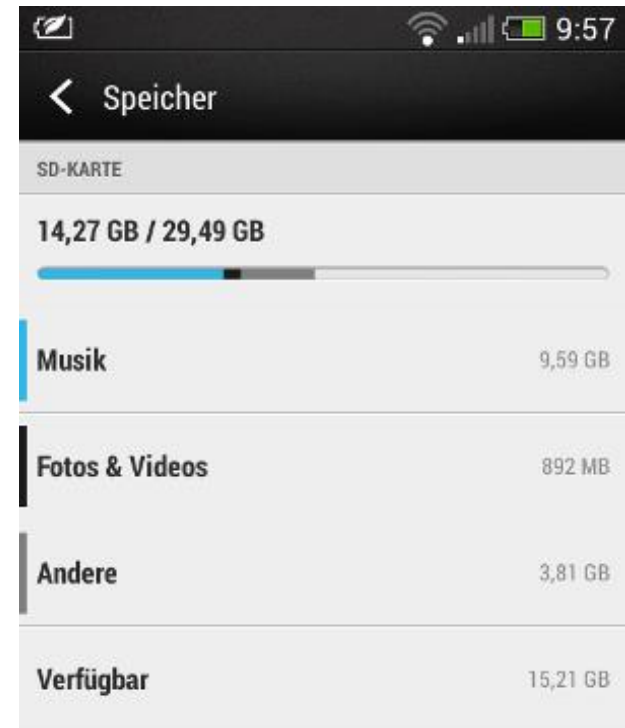
- Interner Speicher
 - App-Speicher, wird nur von Applikationen verwendet
 - kein direkter Benutzerzugriff
 - fest im Telefon verbaut



- Telefonspeicher
 - fest im Telefon verbaut
 - frei zugänglich für Anwendungen und Nutzer (schreiben, löschen)



- Externer Speicher
 - eingesetzte Speicherkarte (SD)
 - vom Benutzer schreib- und lesbar



 *SD Karte*
Secure Digital

- Smartphone-Speicher ist in verschiedene Partitionen eingeteilt.

```

1  rootfs / rootfs ro,relatime 0 0
2  tmpfs /dev tmpfs rw,nosuid,relatime,mode=755 0 0
3  devpts /dev/pts devpts rw,relatime,mode=600 0 0
4  none /dev/cpuctl cgroup rw,relatime,cpu 0 0
5  none /dev/timer_group cgroup rw,relatime,timer_slack 0 0
6  proc /proc proc rw,relatime 0 0
7  sysfs /sys sysfs rw,relatime 0 0
8  none /acct cgroup rw,relatime,cpuacct 0 0
9  tmpfs /mnt/secure tmpfs rw,relatime,mode=700 0 0
10 tmpfs /mnt/obb tmpfs rw,relatime,mode=755,gid=1000 0 0
11 /dev/block/mmcblk0p33 /system ext4 ro,noatime,data=ordered 0 0
12 /dev/block/mmcblk0p35 /data ext4 rw,nosuid,nodev,noatime,discard,noauto_da_alloc
13 DxDrmServerIpc /data/DxDrm/fuse fuse.DxDrmServerIpc rw,nosuid,nodev,relatime
14 /dev/block/mmcblk0p34 /cache ext4 rw,nosuid,nodev,noatime,data=ordered 0 0
15 /dev/block/mmcblk0p25 /devlog ext4 rw,nosuid,nodev,noatime,errors=continue
16 /dev/block/mmcblk0p16 /firmware_radio vfat ro,relatime,fmask=0000,dmask=0000
17 /dev/block/mmcblk0p17 /firmware_q6 vfat ro,relatime,fmask=0000,dmask=0000
18 /dev/block/vold/179:36 /storage/sdcard0 vfat rw,nosuid,nodev,noexec,relatime
19 tmpfs /storage/sdcard0/.android_secure tmpfs ro,relatime,size=0k,mode=000 0 0
20 /dev/block/vold/179:65 /storage/sdcard0/ext_sd vfat rw,dirsync,nosuid,nodev,noexec

```

- Partitionen von Anwendungs- und Cashedaten

Partition	Einhängepunkt	Funktion	Attribute
11	/system	System- und Betriebs-systemdaten	-Lesen -Schreiben
12	/data	Anwendungs- und Be-nutzerdaten	-Lesen -Schreiben
14	/cache	Cache einzelner Anwen-dungen	-Lesen -Schreiben
18	/storage/sdcard0	Telefonspeicher	+Lesen +Schreiben
20	/storage/sdcard0/ext_sd	Externe SD-Karte	+Lesen +Schreiben

Beispiel Einhängepunkte vom HTC One

- Normales Löschen
- Factory-Reset
 - löscht die Partitionen **/data** und **/cache**
 - zusätzliche Option
 - *Alle Daten löschen* – löscht auch den Telefonspeicher
 - *SD-Karte löschen* – löscht externen Speicher
- Überschreiben (endlose Videoaufnahme)
- Kommerzielle Lösungen

Auslese-Software

Name	Hersteller	Version
UFED 4PC	Cellebrite Ltd.	3.0.7.63
Mobile Forensic System XRY	Micro Systemation AB	6.10.1
Android Debug Bridge (ADB)	Google Inc.	1.0.31
Convert and copy a file (dd)	Open Source	8.13

Analyse-Software

Name	Hersteller	Version
UFED Physical Analyzer	Cellebrite Ltd.	3.9.7
XRY Physical	Micro Systemation AB	6.10.1
Internet Evidence Finder	Magnet Forensics Inc.	6.3
Testdisk und PhotoRec	CG Security	6.14
Phone Image Carver	GetData Pty Ltd.	1.6.0.16

Android 4.1.2



Samsung
GT-i9023

Android 4.2.2



HTC
One SV

Android 4.0.3



Sony
ST-25i

iOS 7.1



Apple
iPhone 4S

OS 5



Blackberry
Curve 8520

- 200 Kontakte (597 Telefonbucheinträge)
- 185 SMS
- 60 Anruflisteneinträge
- 800 Bilder (je 5-50 kB)
- 70 Audiodateien (MP3-Daten, je 4-12 MB)

- Image erstellen (1-zu-1 Kopie)
 - Feststellen, dass der Anfangszustand vorhanden ist
- Löschen des Mobiltelefons
- Erneute Untersuchung des Mobiltelefons

- **Kontakte:**
`/data/data/databases/com.android.providers.contacts/contacts2.db`
- **Anrufliste:**
`/data/data/databases/com.android.providers.contacts/calls.db`
- **SMS:**
`/data/data/databases/com.android.providers.telephony/mmssms.db`
- Gelöschte Einträge werden nur als „gelöscht“ markiert und der Speicher wird freigegeben, Daten noch da
- Das gleiche gilt für das Löschen von Bildern und anderen Dateien

- Samsung GT-i9023

Benötigte Zeit	24 Minuten	
Daten	Vor dem Reset	Nach dem Reset
Telefonbucheinträge	597	0
SMS	185	0
Anrufliste	60	0
Bilder	800	791
Audio	70	70

9 gelöschte Bilder wurden vom Betriebssystem überschrieben

- HTC One SV

Benötigte Zeit	35 Minuten	
Daten	Vor dem Reset	Nach dem Reset
Telefonbucheinträge	597	0
SMS	185	0
Anrufliste	60	0
Bilder	800	794
Audio	70	68

6 gelöschte Bilder und 2 Audiodateien wurden vom Betriebssystem überschrieben

- Sony ST-25i

Benötigte Zeit	15 Minuten	
Daten	Vor dem Reset	Nach dem Reset
Telefonbucheinträge	597	299
SMS	185	0
Anrufliste	60	0
Bilder	800	779
Audio	70	69

- Apple iPhone 4S

Benötigte Zeit	57 Minuten	
Daten	Vor dem Reset	Nach dem Reset
Telefonbucheinträge	597	0
SMS	185	0
Anrufliste	60	0
Bilder	800	0
Audio	70	0

- Blackberry Curve 8520

Benötigte Zeit	23 Minuten	
Daten	Vor dem Reset	Nach "Secure Wipe"
Telefonbucheinträge	597	0
SMS	185	0
Anrufliste	60	0
Bilder	50	0
Audio	1	0

Ab Betriebssystemversion 5.0+ Löschfunktion *Secure Wipe*

3. Löschen durch Aufnahme von Videos

- Zuerst muss ein Factory Reset durchgeführt werden
 - der gesamte Speicher muss freigegeben sein
- Kamera hat nicht immer die Berechtigung auf den internen und den Telefonerweiterungsspeicher
 - herstellerabhängig

Es konnten alle Daten gelöscht werden

■ Abhängig von der Auflösung des Videos (16GB)

Form		Dauer
240p	320x240	487,11 Minuten
320p	480x320	162,33 Minuten
480p	640x480	46,61 Minuten
720p	1280x720	13,20 Minuten
1080p	1920x1080	7,95 Minuten

- Secure Wipe
 - die Daten konnten wiederhergestellt werden
- Nuke My Device
 - abgestürzt ohne Fehlermeldung
- iSchredder Pro
 - mehrmaliges Überschreiben (Auswahl)
 - Daten konnten größten Teils wieder hergestellt werden

Alle diese Produkte haben leider kein einziges positives Ergebnis gebracht.

- getestet mit Android 4.0.3+ („Ice Cream Sandwich“)
- Keine Root-Rechte
- Die Partition kann ausgewählt werden
 - interner und externer Speicher
- Schreibblockgröße kann ausgewählt werden
- Die Anwendung ist absturzsicher

Bitte stellen Sie sicher, dass Sie Ihr Smartphone auf die Werkseinstellungen zurückgesetzt haben!

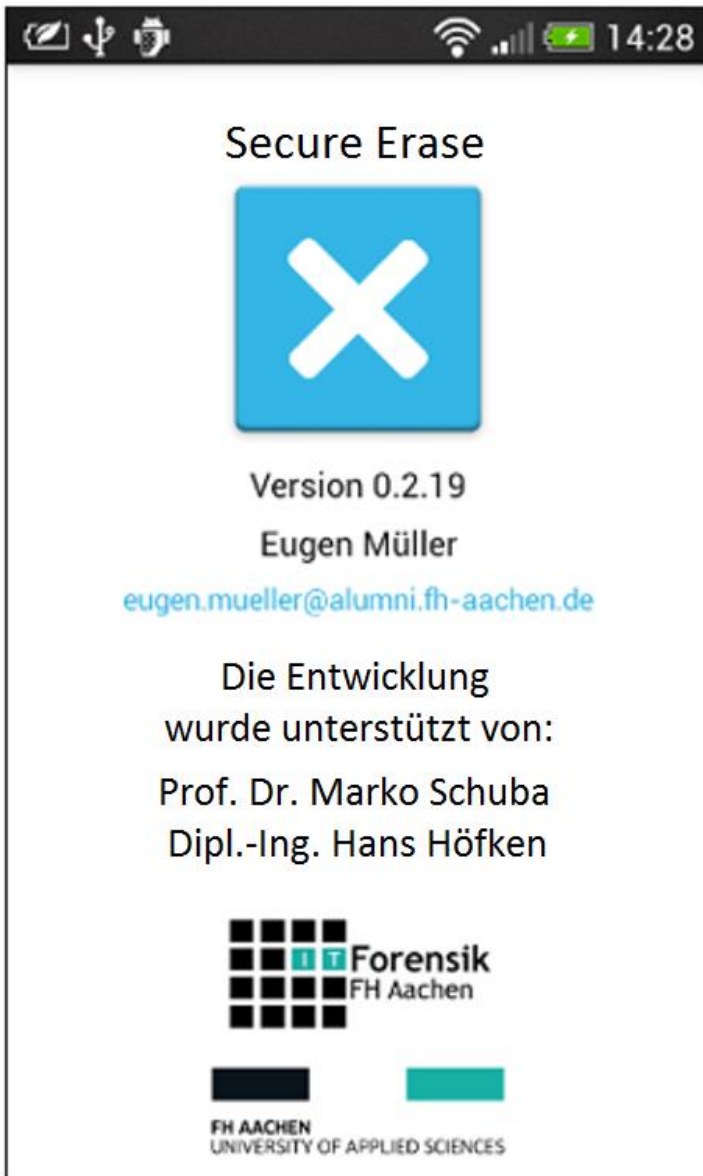
Sind Sie sicher, dass Sie den gesamten freien Speicher über...

Es

Abbr

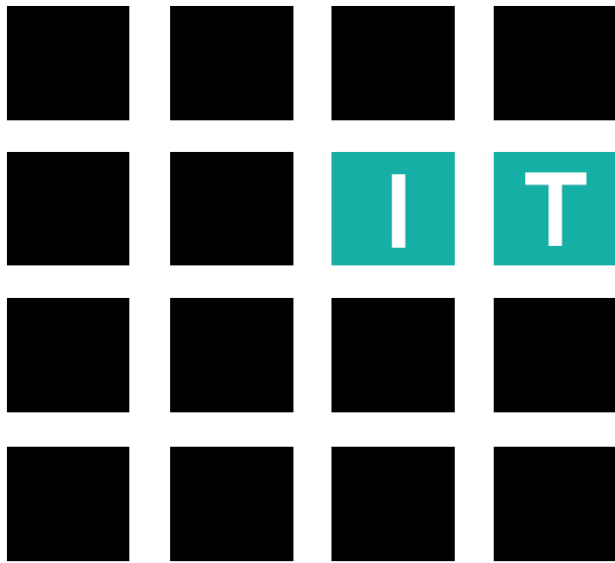
Es konnten alle Daten gelöscht werden





Download unter
www.it-forensik.fh-aachen.de
im Projektbereich





Forensik
FH Aachen

Vielen Dank für Ihre Aufmerksamkeit

? Fragen