Erasure Verification on Flash Memory

Is the data really gone?

Will DeLisi and Josey Santana

Flash Memory Summit

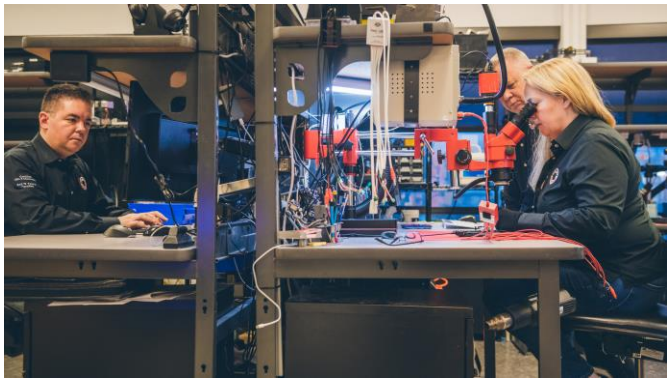
Presenter Company / Organization

DriveSavers Inc.

Flash Memory Summit

Overview

- Levels of data erasure verification
- Trim and Garbage Collection
- Case Studies
- Compliance and erasure verification
- Recommendations



Flash Memory Summit

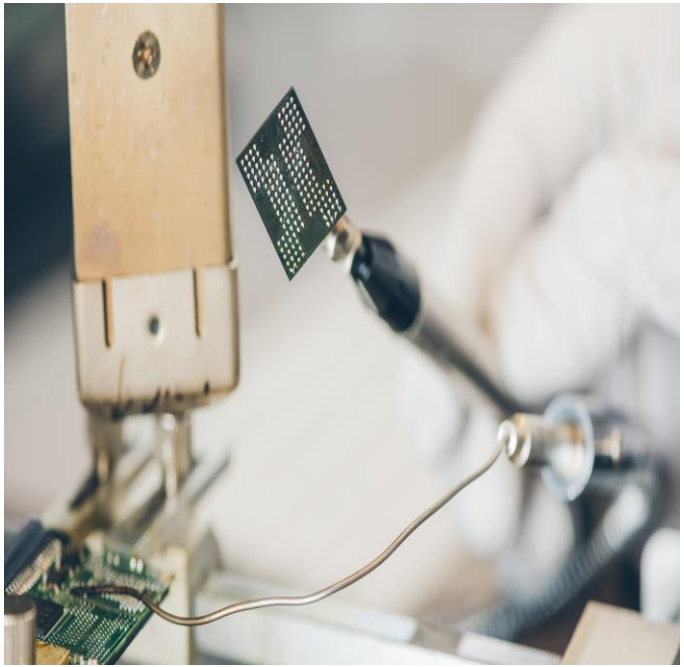
Abstract

When it's time to move on from a flash storage device, whether it's due to device failure or a standard hardware upgrade, of course you erase the data from that device before disposing of it or repurposing it.

But what if some of that data is still there at a deeper level?

What might happen if customer data, intellectual property or other sensitive data ended up in the wrong hands?

We will paint the picture of the difference between a Level 1 erasure verification versus a Level 2 and why it matters to clients that want to be sure that data is erased.



NIST Standards

National Institute of Standards and Technology

- Level 1 = Clear
- Level 2 = Purge
- Level 3 = Destroy

Levels of Data Erasure Verification

- Level 1 erasure verification “clear”
  - Overwriting storage space with non-sensitive data.
- Level 2 “purge” erasure verification
  - Degaussing and executing the firmware Secure Erase command (for ATA drives only)
  - Utilize bitmap graphics, encryption vs XOR

NAND Chip Off Eligible

Common Applications:

- SD cards
- MicroSD cards
- Compact Flash Cards
- CFast cards
- SSDs

Popular NAND Brands

- Toshiba
- Silicon Motion
- Hynix
- SanDisk
- Intel

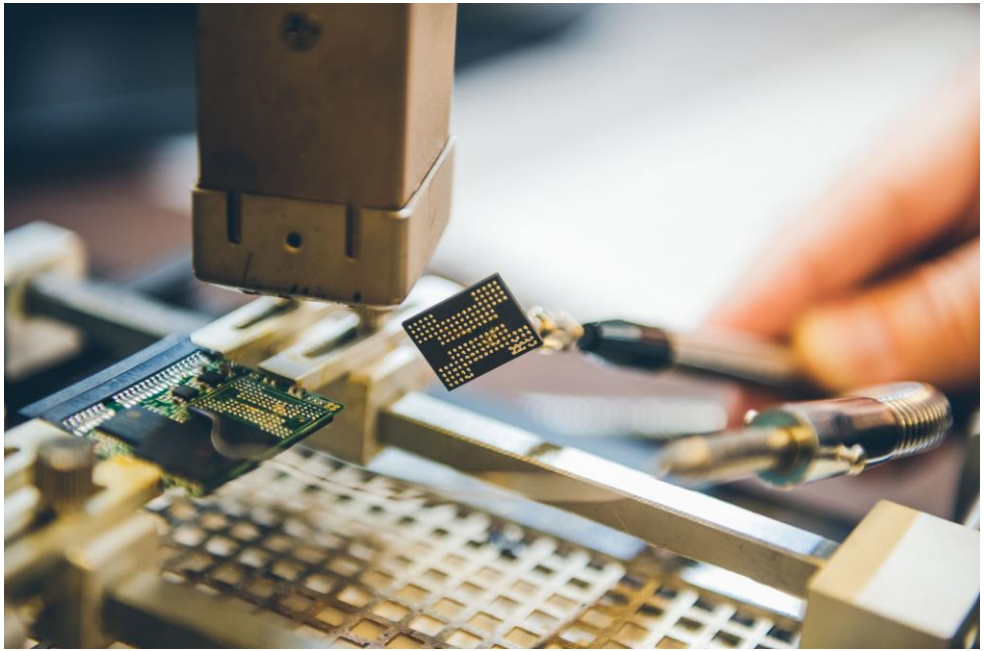
Controller Functions

- Translation Tables
- Wear Leveling
- ECC - Error Correction
- XOR
- Page Allocation
- Garbage Collection w/ TRIM

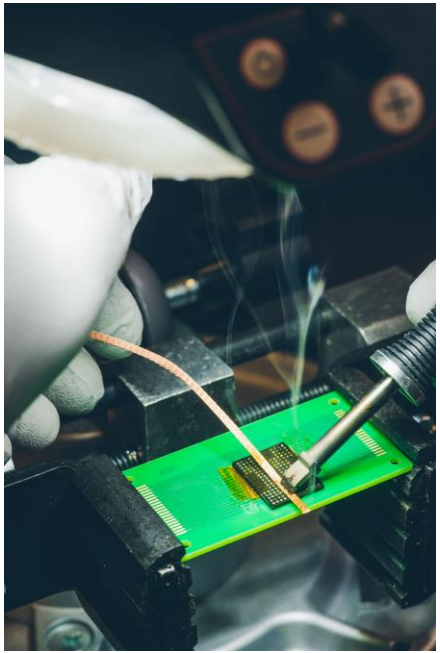
Case Study

- Chip Off Recovery from CFast Card
- 256GB Lexar CFast card.
- End user reformatted the card by mistake.
- No user data recoverable using Level 1 - Clear methods.

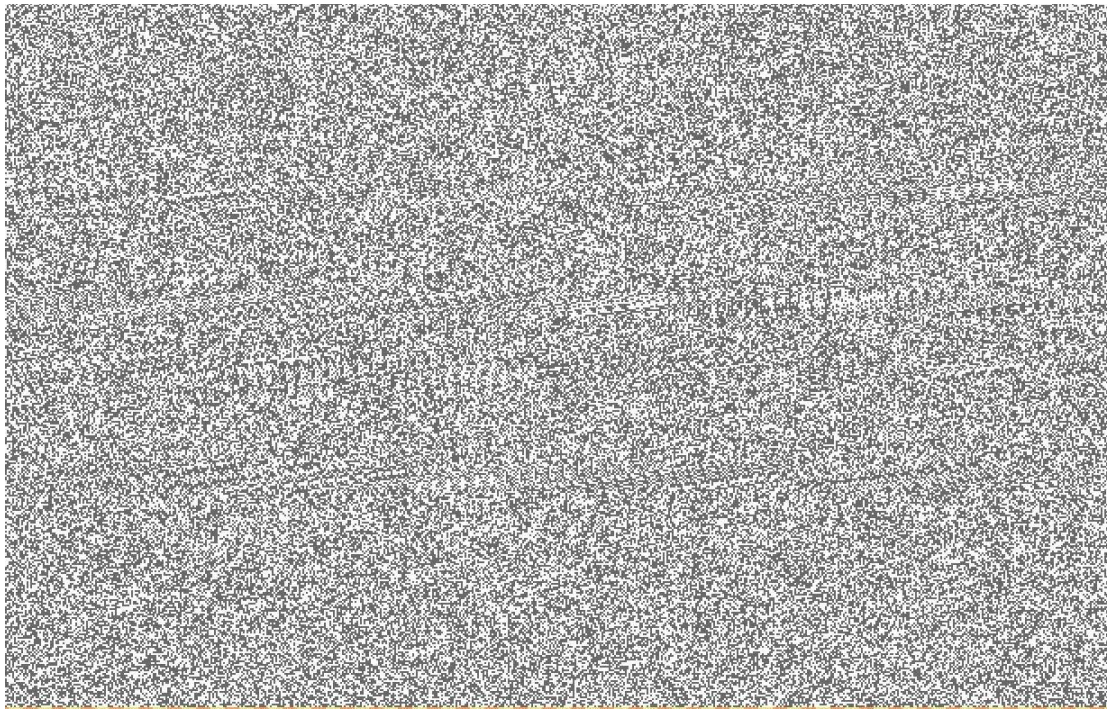
Chip removal using infrared heating source.



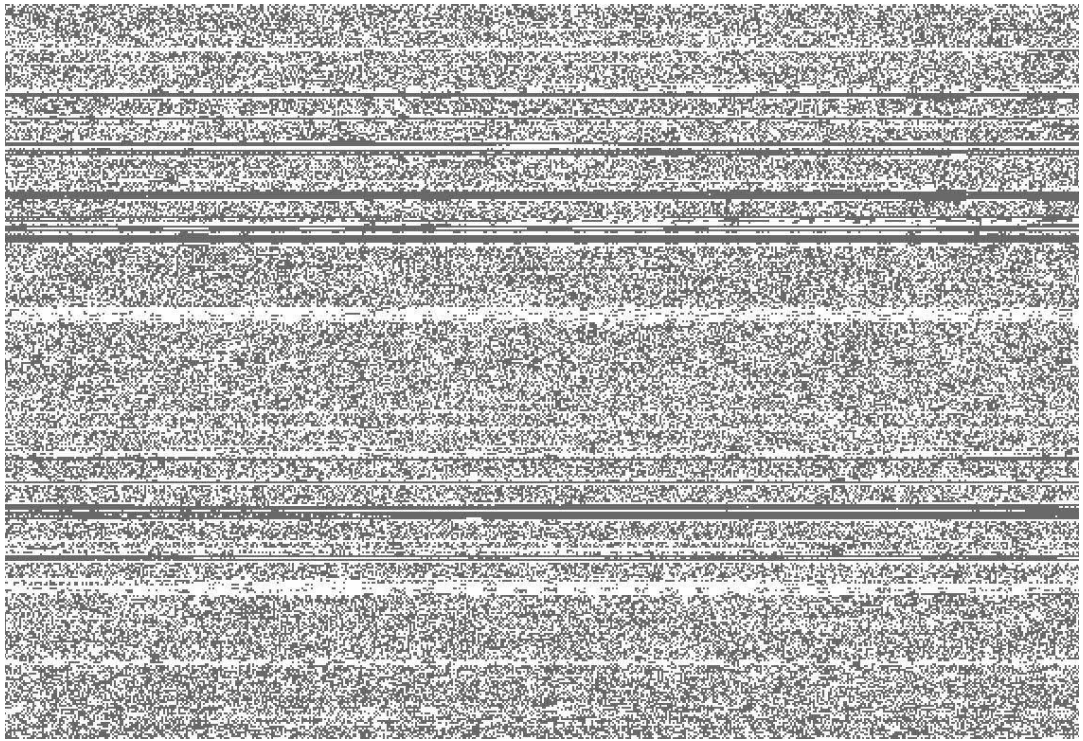
Chip preparation.



XORed Data

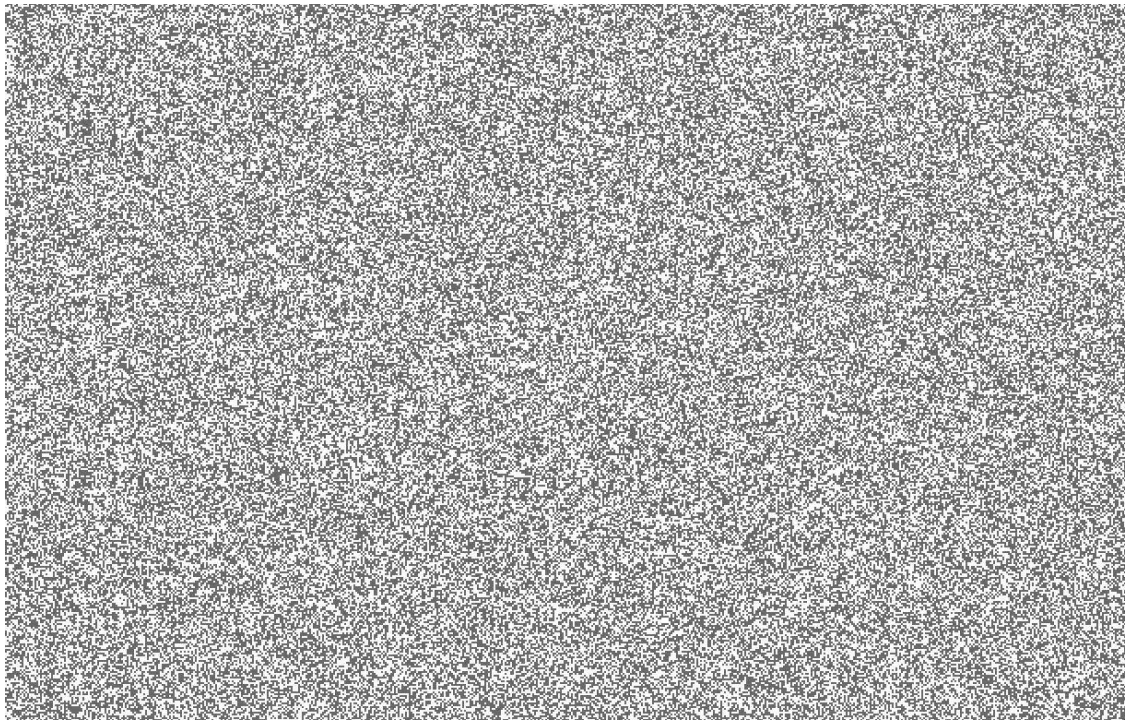


Data Without XOR or Any Encryption



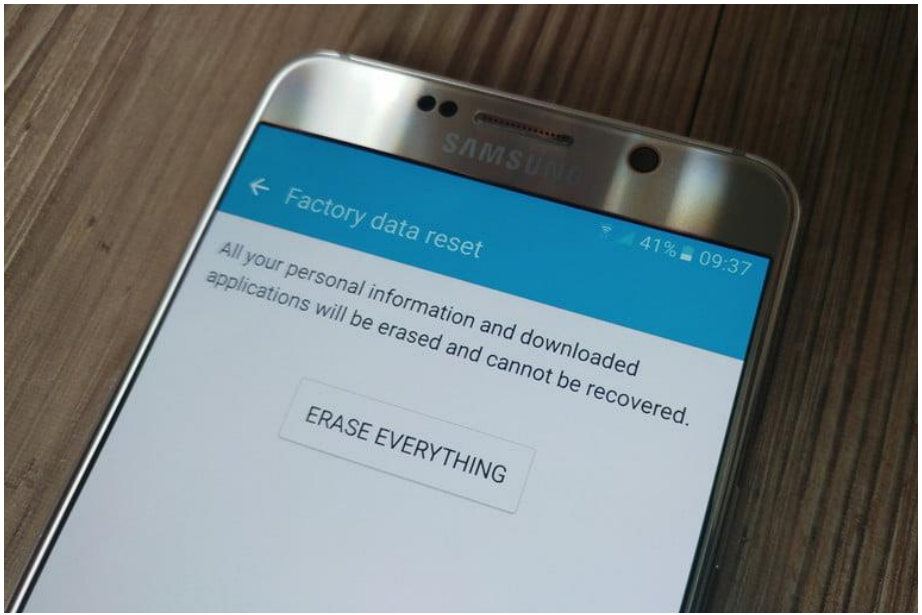
Flash Memory Summit

Data in Encrypted Form



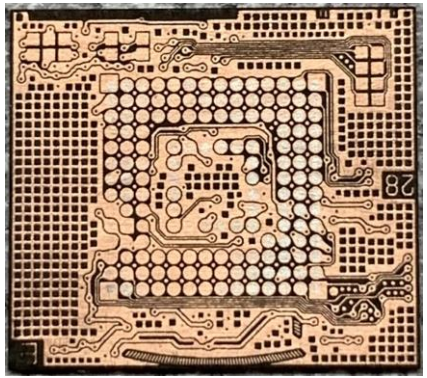
Case Study

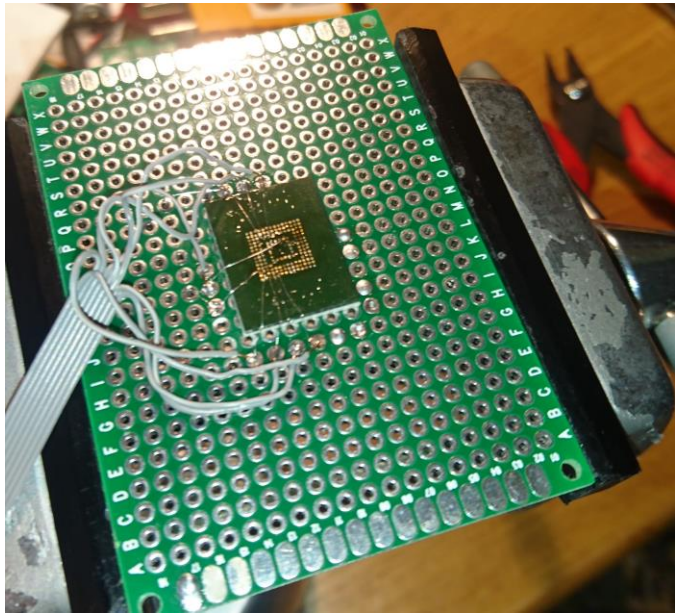
- Erasure Verification
- eMMC from a Samsung Galaxy
- Level 1 – Clear – Client uses proprietary software to securely erase device
- Pulled physical image from device using forensic tools to verify Level 1 – Clear Verification. All 00s at logical level



Flash Memory Summit

- Level 2 – Purge – Pull low level image to determine Erasure
- Wired to logic analyzer to identify pinout
- Wired to NAND flash reader
- Created proper configuration for NAND
- Read NAND for raw image
- Extracted XOR, built ECC (BCH) layout
- Reconstructed blocks to create logical image
- Extracted Android databases and other data





Data recovered after proprietary erasure software

Read	Type	Folder	Timestamp (UTC+0)	From	To	Message
no	**SMS**	**Inbox**	**09.04.2018 6:36:07**	[redacted]		**Message 2: received**
yes	SMS	Sent	09.04.2018 6:34:59			Monday message 2 to Jennifer
yes	SMS	Outbox	09.04.2018 6:34:57			Monday message 2 to Jennifer
yes	SMS	Sent	09.04.2018 6:31:22			Monday message to Jennifer
yes	SMS	Sent	09.04.2018 6:31:21			Monday message to Jennifer
yes	SMS	Sent	06.04.2018 7:15:38			To have the .db files with some info
yes	SMS	Sent	06.04.2018 7:15:37			To have the .db files with some info
yes	SMS	Sent	06.04.2018 7:15:12			Simply logs
yes	SMS	Sent	06.04.2018 7:15:10			Simply logs
yes	SMS	Drafts	06.04.2018 7:05:35			DriveSavers Samsung Galaxy S4
yes	SMS	Drafts	06.04.2018 7:05:08			DriveSavers Galaxy S4
yes	SMS	Drafts	06.04.2018 7:04:22			DriveSavers S4
yes	SMS	Drafts	06.04.2018 7:03:41			DriveSavers
yes	SMS	Inbox	06.04.2018 6:56:39			WhatsApp code 981-718. You can also tap on this link to verify your phone: v.whatsapp.com/981718

Data recovered from previous use

Read	Type	Folder	Timestamp (UTC+0)	From	To	Message
unknown	SMS	Inbox	18.08.2016 8:43:59			Vodafone Mailbox: +567946446947 hat keine Nachric
unknown	SMS	Inbox	17.08.2016 17:14:28			Vodafone Mailbox: +569746568464 hat keine Nachrich
unknown	SMS	Sent	16.08.2016 5:58:30			Morgen :) is noch gar noch ganz fertsch....
unknown	SMS	Inbox	15.08.2016 16:14:26			Huhu, ich weiß, bin ne Nervensäge 😀 kannst du das
unknown	SMS	Inbox	15.08.2016 13:35:57			Sehr geehrter Kunde, gern stellen wir Ihren Wunsch
unknown	SMS	Inbox	14.08.2016 16:55:36			Die TAN für die Einzelüberweisung vom 14.08.2016 1
unknown	SMS	Inbox	14.08.2016 9:54:20			Roaming in der EU: Sollten Sie in Ihrem nationalen
unknown	SMS	Inbox	14.08.2016 9:42:43			Lieber Kunde, willkommen in Tschechien! Mit Ihrem
unknown	SMS	Inbox	13.08.2016 12:49:41			Vodafone Mailbox: +564845456464 hat keine Nachric
unknown	SMS	Inbox	13.08.2016 12:26:16			Vodafone Mailbox: +569435467464 hat keine Nachric
unknown	SMS	Inbox	13.08.2016 11:20:54			Huhu, stehst wieder an der Strasse, damit ich weiß
unknown	SMS	Sent	13.08.2016 4:02:42			Jetz alles gut
unknown	SMS	Inbox	13.08.2016 3:51:05			Wasn los :)
unknown	SMS	Inbox	12.08.2016 13:40:10			0*******7
unknown	SMS	Inbox	12.08.2016 2:24:25			Wat brennt denn? Oo
unknown	SMS	Sent	11.08.2016 21:13:23			Ey der flo hier. ...
unknown	SMS	Sent	11.08.2016 9:04:00			Hey dich gibt's ja a noch, danke meiner
unknown	SMS	Inbox	11.08.2016 8:20:35			Grüße wünsch dir alles gute zum geburtstag altes h

Data recovered from previous use

yes	**no**	**SMS**	**Inbox**	**08.08.2016 13:31:45**	[redacted]	**Die TAN für die Einzelüberweisung vom 08.08.2016 15:31:41 über 39,35 EUR auf die IBAN ***3*******3 lautet: 751128**	**Carver**
yes	unknown	SMS	Inbox	07.08.2016 17:23:14		WhatsApp code 221-917. Du kannst auch auf diesen	Carver
yes	yes	SMS	Inbox	29.04.2016 12:38:38		Alles klae dann Sonntag der 22.5 10 Uhr bei mir	Carver
yes	yes	SMS	Sent	29.04.2016 12:38:02		Ok. Kein Problem 😊	Carver
yes	yes	SMS	Inbox	29.04.2016 12:35:17		So hab mit Lisa gesprochen nächste Woche Sonntag ubd darauf kann sie nicht. Am 22.5 um 10 Uhr geht ok?	Carver
yes	yes	SMS	Sent	28.04.2016 14:43:46		Vehling hier	Carver
yes	yes	SMS	Sent	27.04.2016 3:49:13		Ich weiß schon, warum ich nachts mein Handy aus mache. Ich muss nämlich arbeiten 😨	Carver
yes	yes	SMS	Inbox	27.04.2016 3:18:39		Kostenfreie Anruf-Info: Der Anrufer +561******4 hat am 27.04. 02:54 Uhr versucht, Sie zu erreichen.	Carver
yes	yes	SMS	Sent	26.04.2016 14:41:57		Vehling hier	Carver
yes	yes	SMS	Inbox	19.04.2016 13:54:06		Kein Stress	Carver
yes	yes	SMS	Sent	19.04.2016 13:53:47		Ich melde mich später	Carver
yes	yes	SMS	Inbox	18.04.2016 15:28:30		Anruf-Info vom 18.04., 17:27 Uhr: +491771488546 ist jetzt wieder erreichbar. Dieser Service ist kostenfrei.	Carver
yes	yes	SMS	Inbox	18.04.2016 15:22:36		Anruf-Info vom 18.04., 17:21 Uhr: +491771488546 ist jetzt wieder erreichbar. Dieser Service ist kostenfrei.	Carver

Data recovered from previous use

yes	yes	SMS	Inbox	18.04.2016 10:22:21	[redacted]	Wir benötigen für den Zeitraum bis zum 03.04.2016 eine Bescheinigung für den Lohnsteuerabzug damit Sie nicht in Sudh 6 abgerechnet werden. *good to k
yes	yes	SMS	Inbox	16.04.2016 9:20:27		Die TAN für die Einzelüberweisung vom 16.04.2016 11:20:20 über 9,74 EUR auf die IBAN ***0******00 lautet: 56***34
yes	yes	SMS	Inbox	15.04.2016 13:56:37		Die TAN für die Einzelüberweisung vom 15.04.2016 15:56:33 über 300,00 EUR auf die IBAN *********34 lautet: 65****
yes	yes	SMS	Inbox	15.04.2016 9:29:57		Ich hab dir das Geld zurück überwiesen. Du kannst mor nicht einfach was überweisen du bringst mich damit in Schwierigkeiten weil ich dann zusehen kann wie ich das nächsten Monat ans amt bezahle.
yes	yes	SMS	Sent	15.04.2016 9:06:33		Bin arbeiten
yes	yes	SMS	Inbox	15.04.2016 9:03:32		Kannst du mir jetzt mal ne Antwort geben wer dir dad gesagt hat das du das überweisen sollst?? Sonst überweise ich das wieder zurück
yes	yes	SMS	Inbox	15.04.2016 6:52:32		Ja hast du n schreiven bekommen wieviel ubd so? Ich nämlich nicht
yes	yes	SMS	Inbox	15.04.2016 6:52:12		Ich habe doch den Vorschuss beantragt das läufz doch über das jungendamt du kannst mir doch nicht einfach
yes	yes	SMS	Sent	15.04.2016 6:51:48		Das muss ich Alles Gut
yes	yes	SMS	Inbox	15.04.2016 6:50:26		Das geht doch über das jungendamt woe kommst du da jetzt auf einmal drauf. Das muss doch mit dem job center abgesprochen werden

Reasons for Erasure Verification

- HIPPA Compliance, company secrets, proprietary data, etc.
- Proprietary in house erasure method verification. Device reuse
- Companies NEED to know their erasure methods are in compliance with NIST and their clients expectation of privacy

Garbage Collection w/ TRIM

- When TRIM is working properly, data should be gone.
- Need Erasure Verification Service to ensure erasure methods and/or TRIM is actually working as expected per controller model
- Many controller models or versions have arbitrary erasure methods

Recommendations

- End-users and businesses
  - Encryption on top to ensure better chance of leaving no plain text at chip-level.
    - Methods of encryption, BitLocker, PGP, File Vault, Checkpoint, etc.
    - Controller manufacturers ensure secure erasure methods are in compliance with NIST standards

Flash Memory Summit

Thank You!

Questions?