SMS recovery from NAND memory of erased eMMC chip

Sasha Sheremetov – CTO of Rusolut

Flash Memory Summit 2017
Santa Clara, CA

WHY ERASE EMMC CHIP

In this experiment the eMMC was intentionally erased (zeroed 0x00) through standard interface in order to prove/disprove existance of after-erase data remnants beyound controller in NAND memory. The SMS messages were selected as a subject of research as a most common and relatively short type of data on smartphones.

REAL WORLD APPLICATION

If we can prove that controller does not erase all the blocks of NAND memory even in extreme situation when device is wiped, it opens a huge potential of recovering old data that was deleted by user but still remained in NAND.

BENEFITS

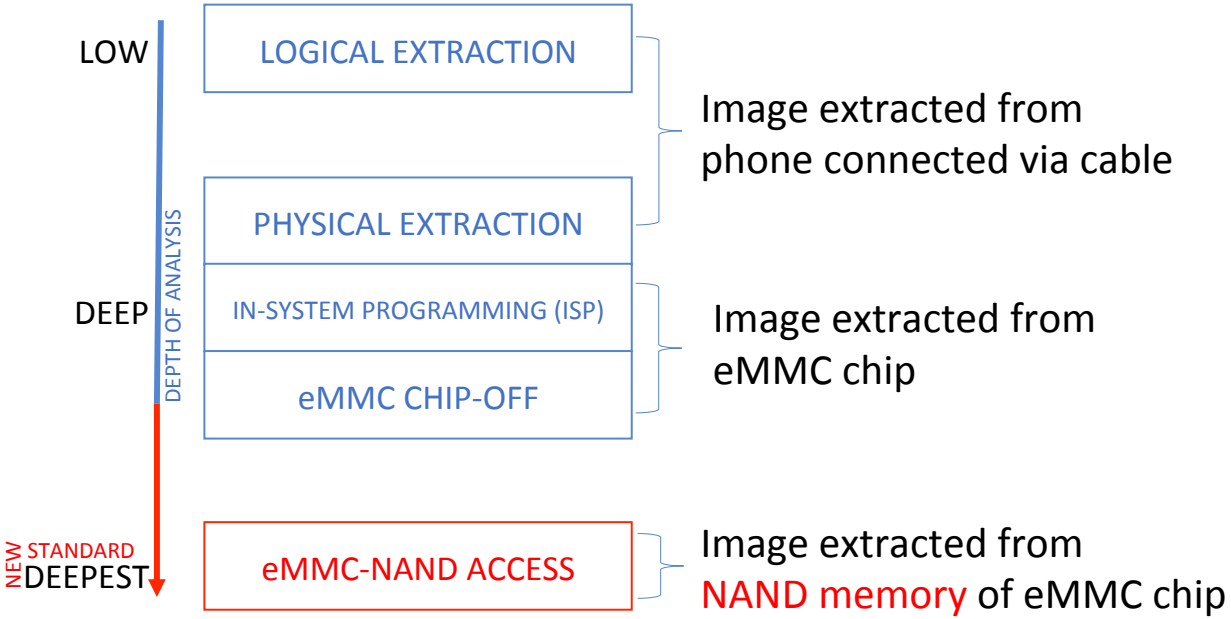
DATA RECOVERY

- data recovery of lost or deleted data in case if no desired files found in eMMC
- data recovery via direct access to NAND memory of damaged eMMC (when controller failed to start up and device is not reacting on commands)

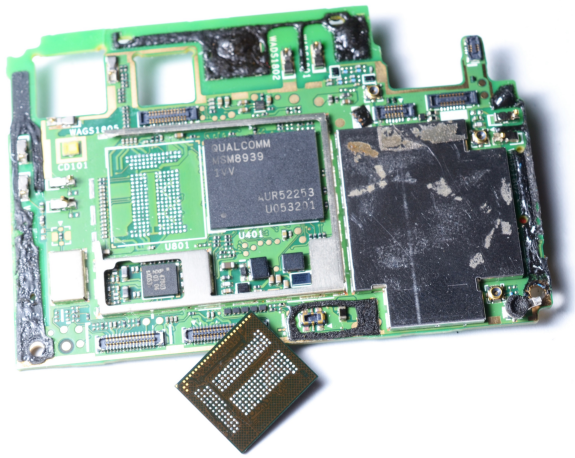
DIGITAL FORENSICS

- retrieval of deleted text messages, chats , etc. on much deeper level that is not accessible for classic mobile forensic tools.

DIFFERENT WAYS OF DATA EXTRACTION AND ANALYSIS FROM ANDROID SMARTPHONES

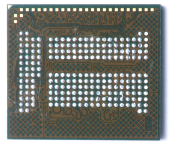


CLASSIC CHIP-OFF AND DATA EXTRACTION FROM eMMC CHIP

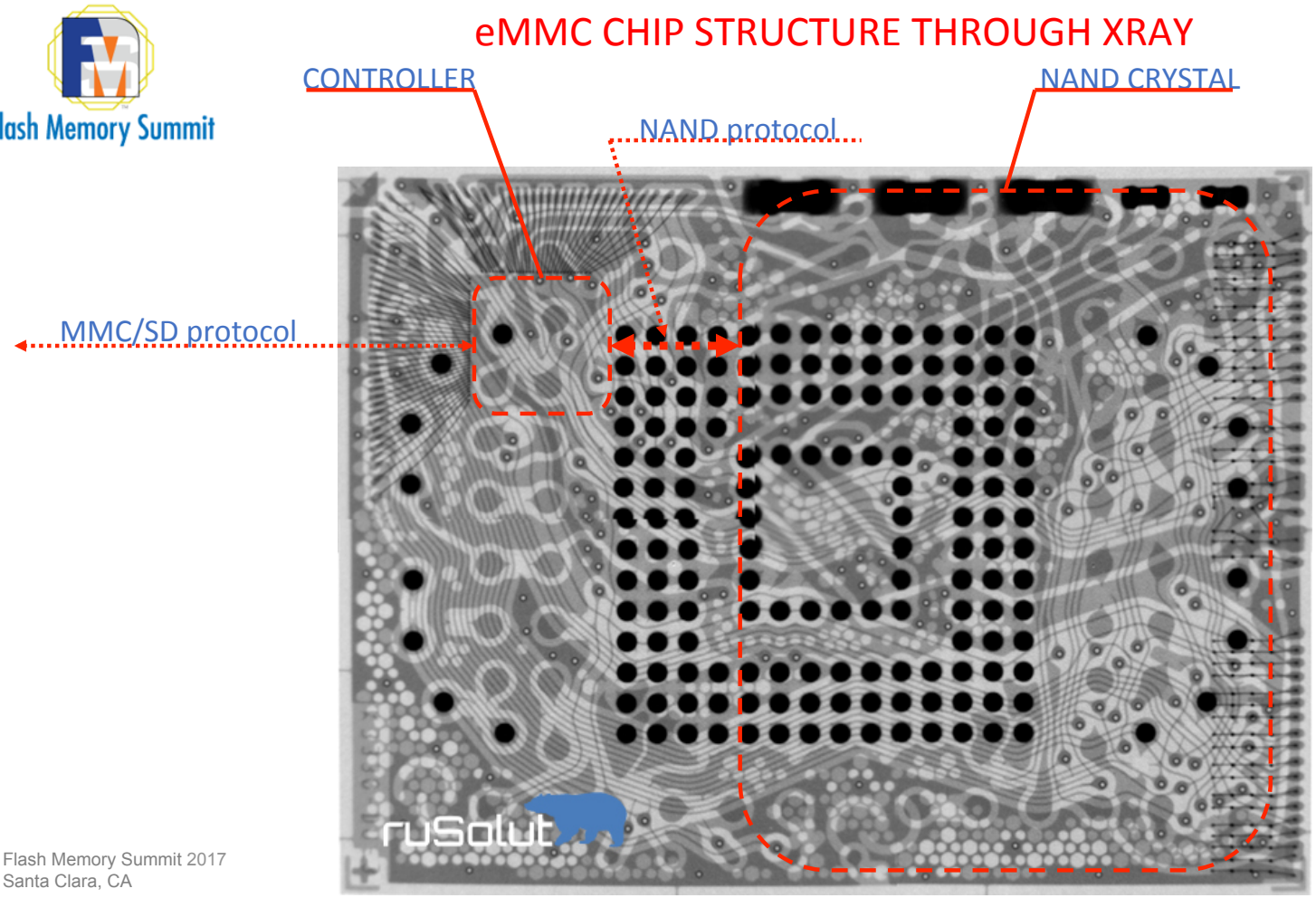


UNSOLDERING

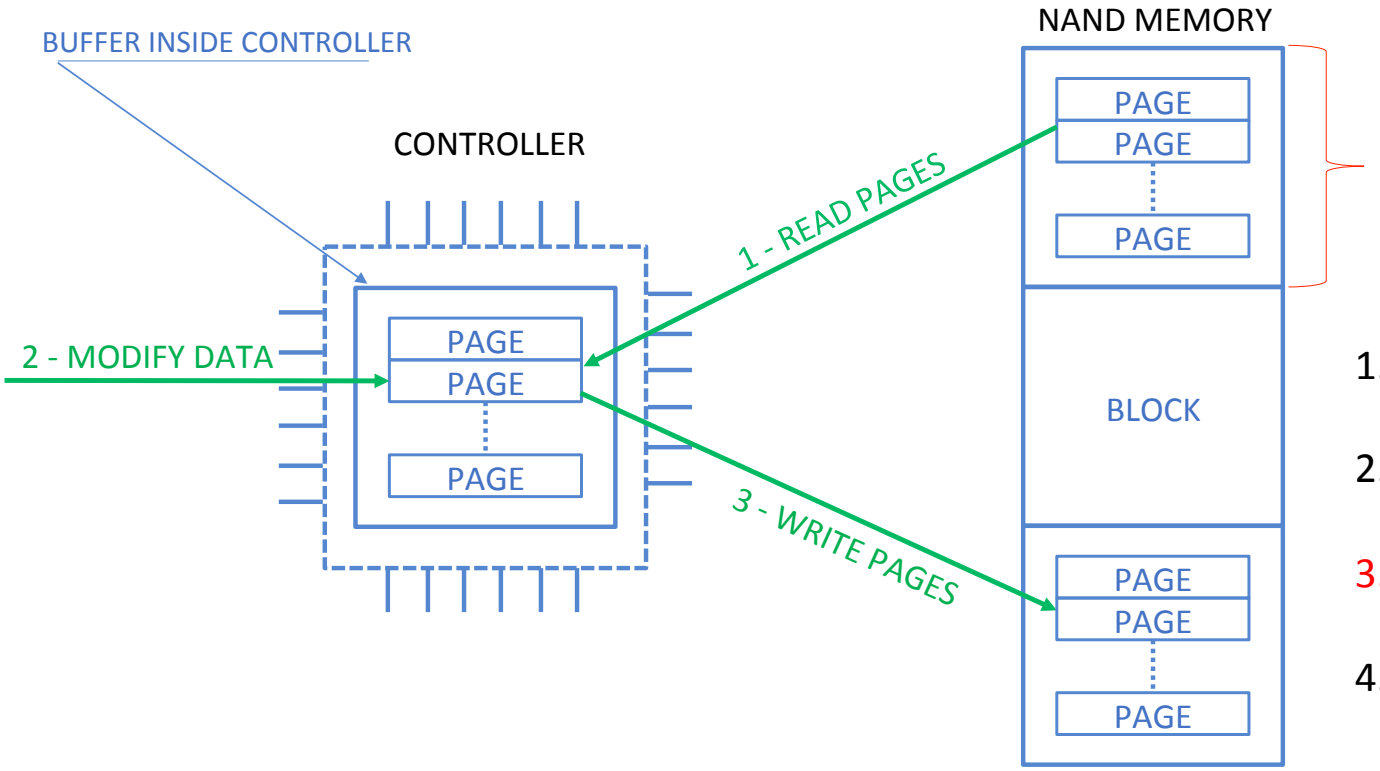
CLEANING



PHYSICAL IMAGE EXTRACTION


Flash Memory Summit
eMMC CHIP STRUCTURE THROUGH XRAY
CONTROLLER
NAND protocol
NAND CRYSTAL
MMC/SD protocol
ruSolut
eMMC = RAW NAND + CONTROLLER

HOW DATA MODIFICATION PROCESS WORKS IN NAND MEMORY



OLD UNERASED BLOCK STAYS UNTOUCHED FOR SOME TIME UNTIL GARBAGE COLLECTION ALGORITHM ERASE IT. USUALLY IT'S NOT SO FAST PROCESS

1. READ PAGES
2. MODIFY DATA
3. ~~ERASE BLOCK~~
4. PROGRAM (WRITE) PAGES TO ANOTHER BLOCK

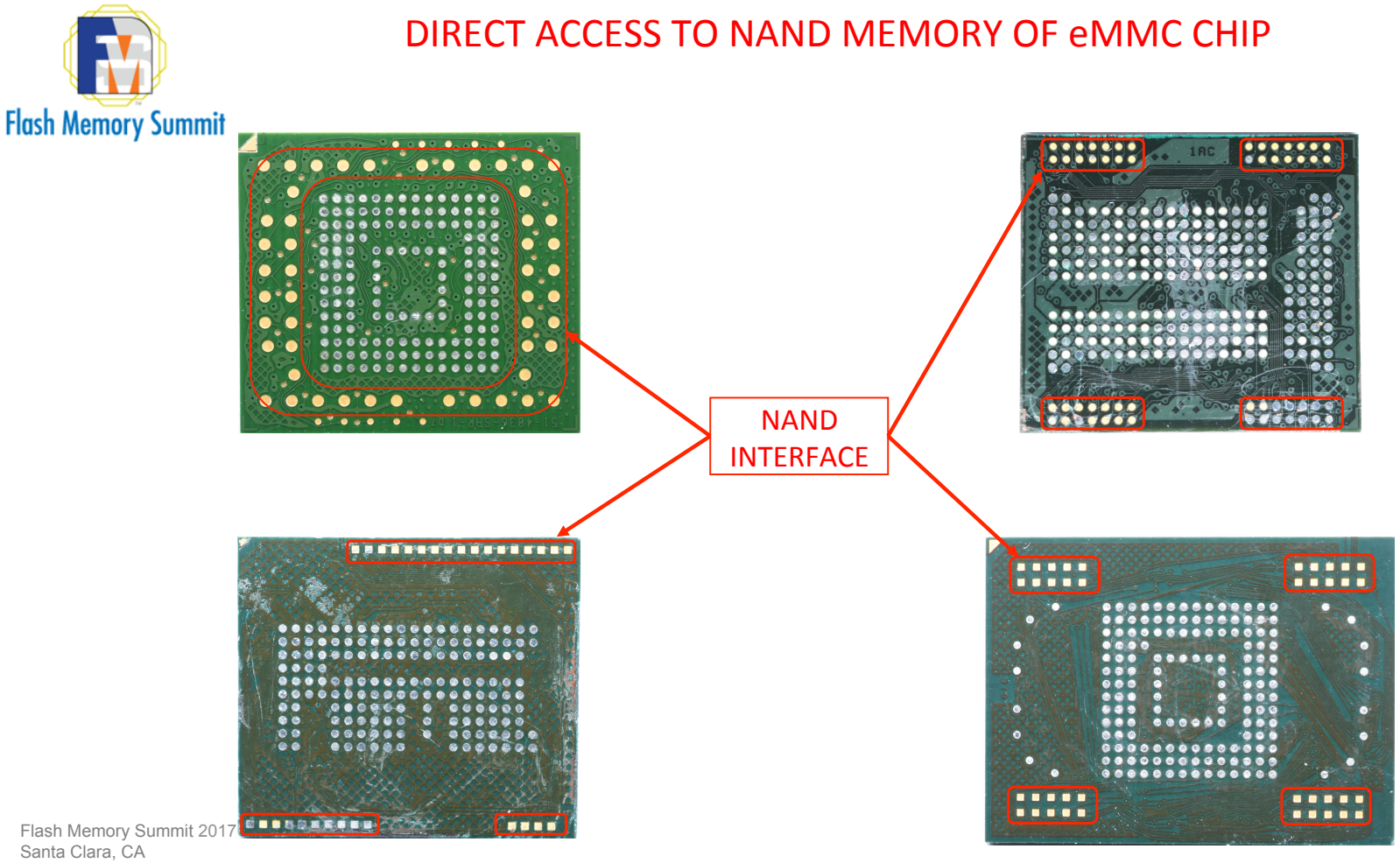
LET'S TRY TO EXTRACT SOME DELETED SMS FROM THOSE "OVERWRITTEN" GARBAGE BLOCKS OF eMMC MEMORY VIA NAND INTERFACE

TO MAKE THINGS WORSE LET'S ERASE EMMC CHIP!

Flash Memory Summit 2017
Santa Clara, CA

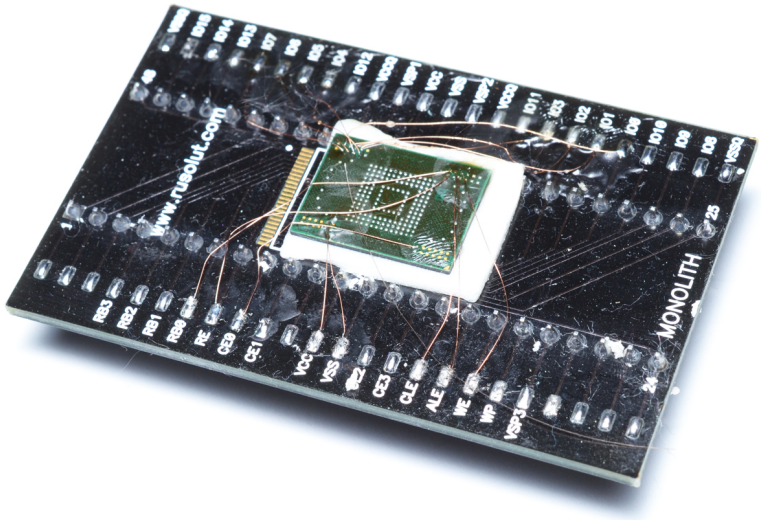
THE DATA EXTRACTION ALGORITHM

- GAIN ACCESS TO NAND MEMORY OF eMMC CHIP
- EXTRACT PHYSICAL IMAGE OF NAND CHIP
- DECODE PHYSICAL IMAGE TO READABLE FORM
- CHECK IF THERE ARE STILL BLOCKS WITH “REMNANTS” IN THE DUMP (WE EXPECT TO SEE 0x00 IN THE WHOLE DUMP)
- SCAN DUMP USING SQLITE CARVING ALGORITHM TO FIND DELETED SMS
- ANALYSE RESULTS (WE EXPECT TO FIND ~~NOTHING!~~ USER’S DATA)

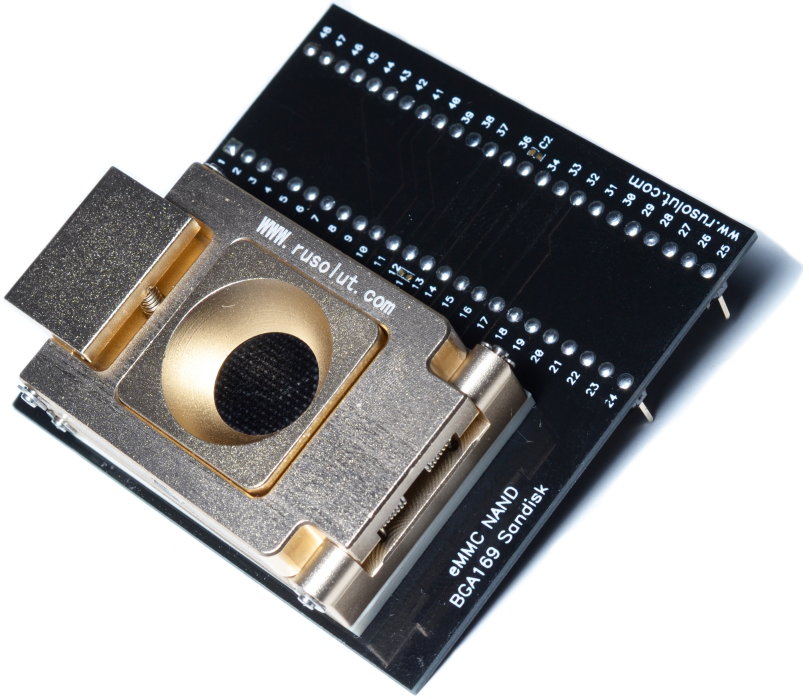

DIRECT ACCESS TO NAND MEMORY OF eMMC CHIP
NAND
INTERFACE

eMMC CHIP ON ADAPTER CONNECTED VIA NAND PROTOCOL

COMPLICATED WAY

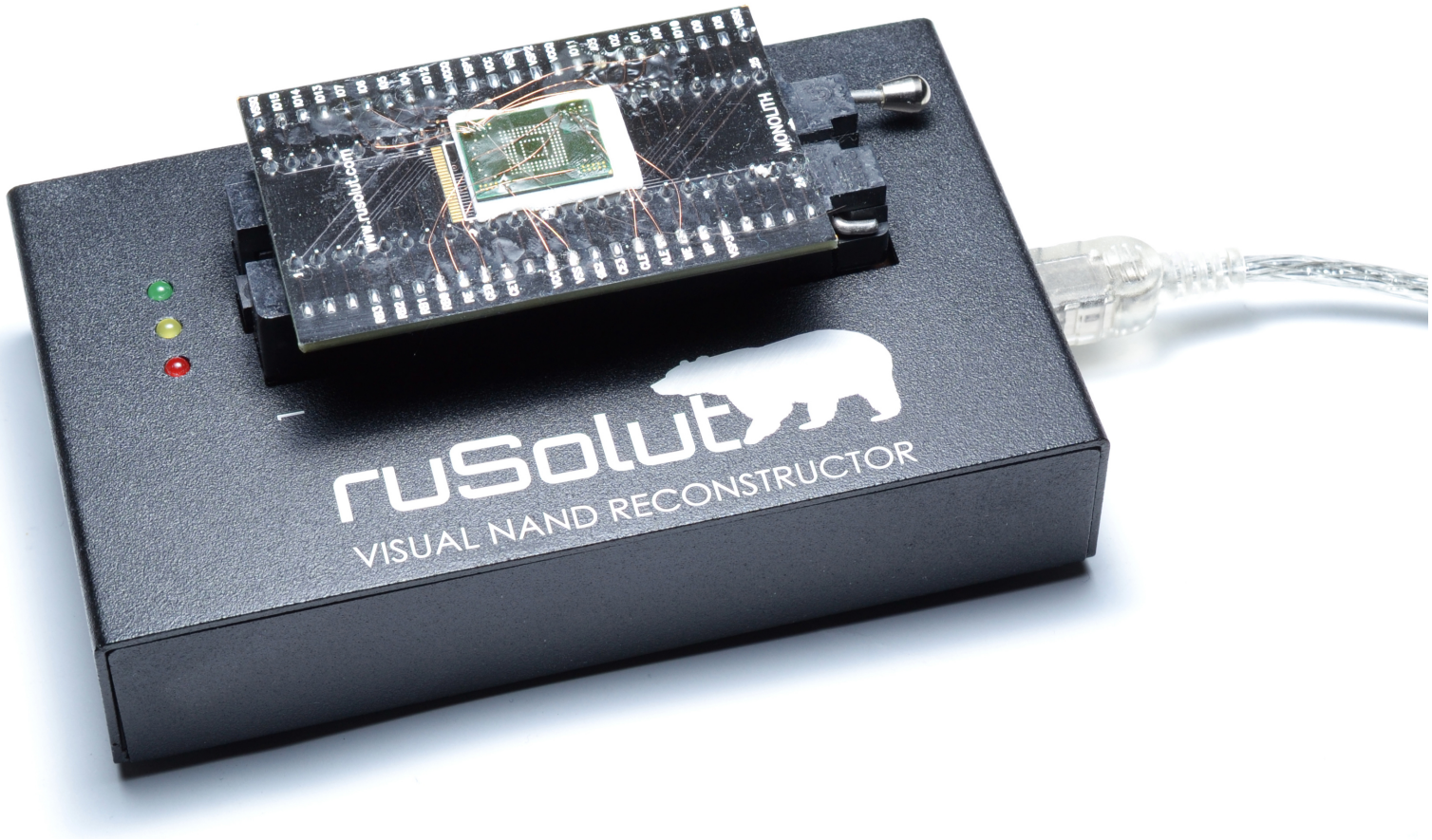


EASY WAY



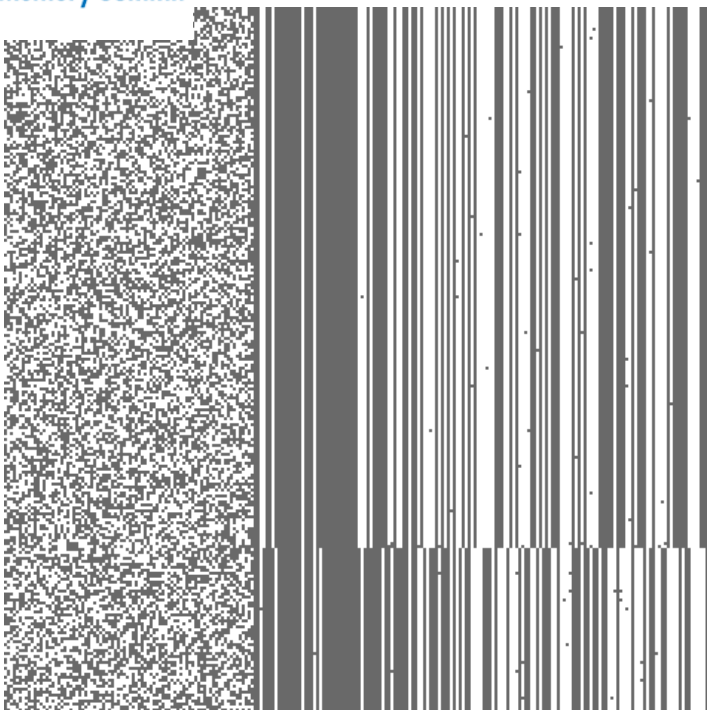
Flash Memory Summit

ADAPTER MOUNTED INTO NAND READER FOR FURTHER PHYSICAL IMAGE (RAW DUMP) EXTRACTION

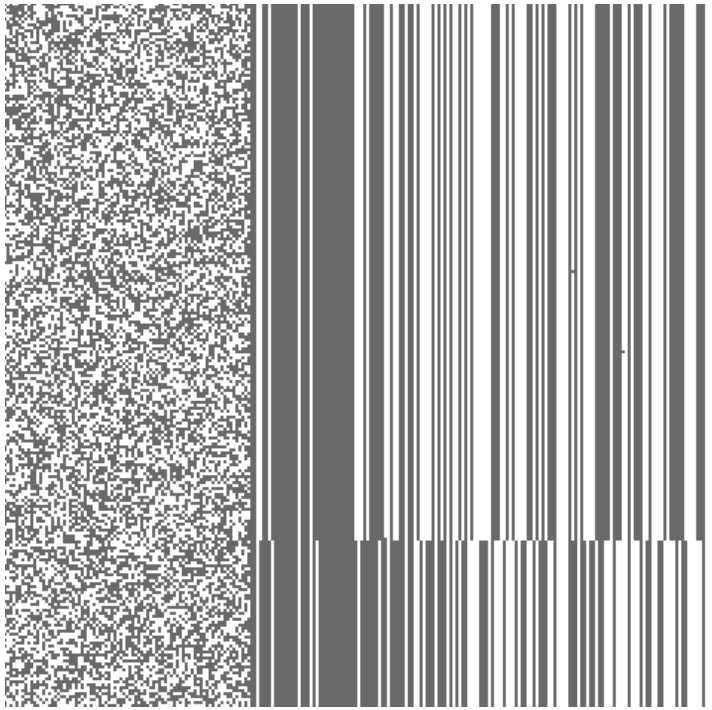


BIT ERRORS AND ECC CORRECTION

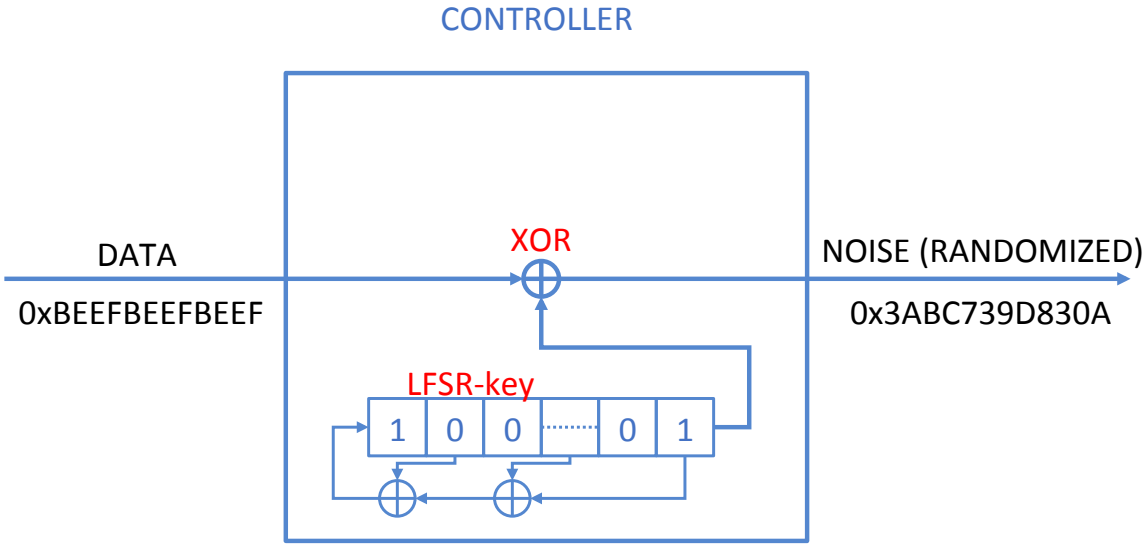
BEFORE ECC



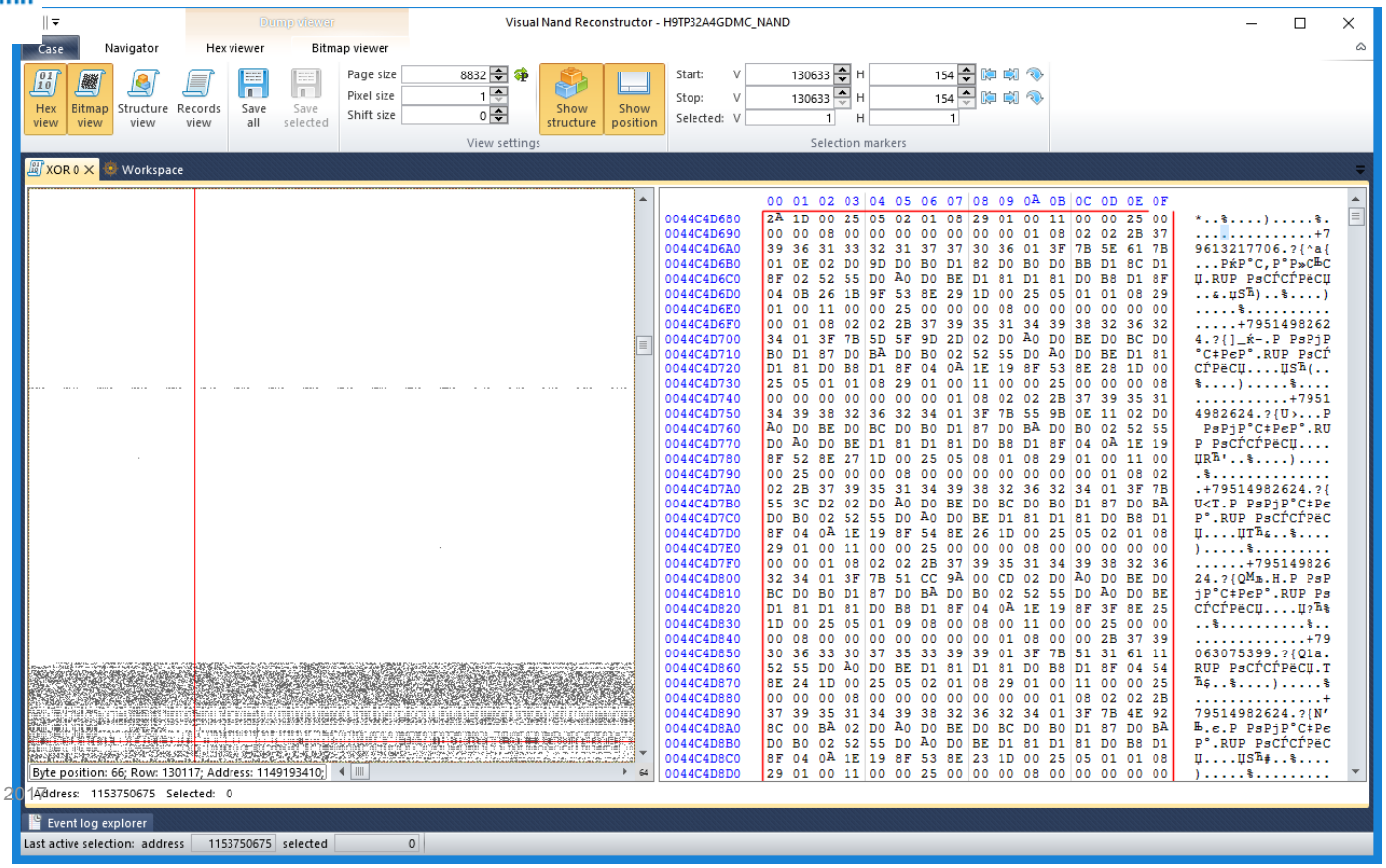
AFTER ECC



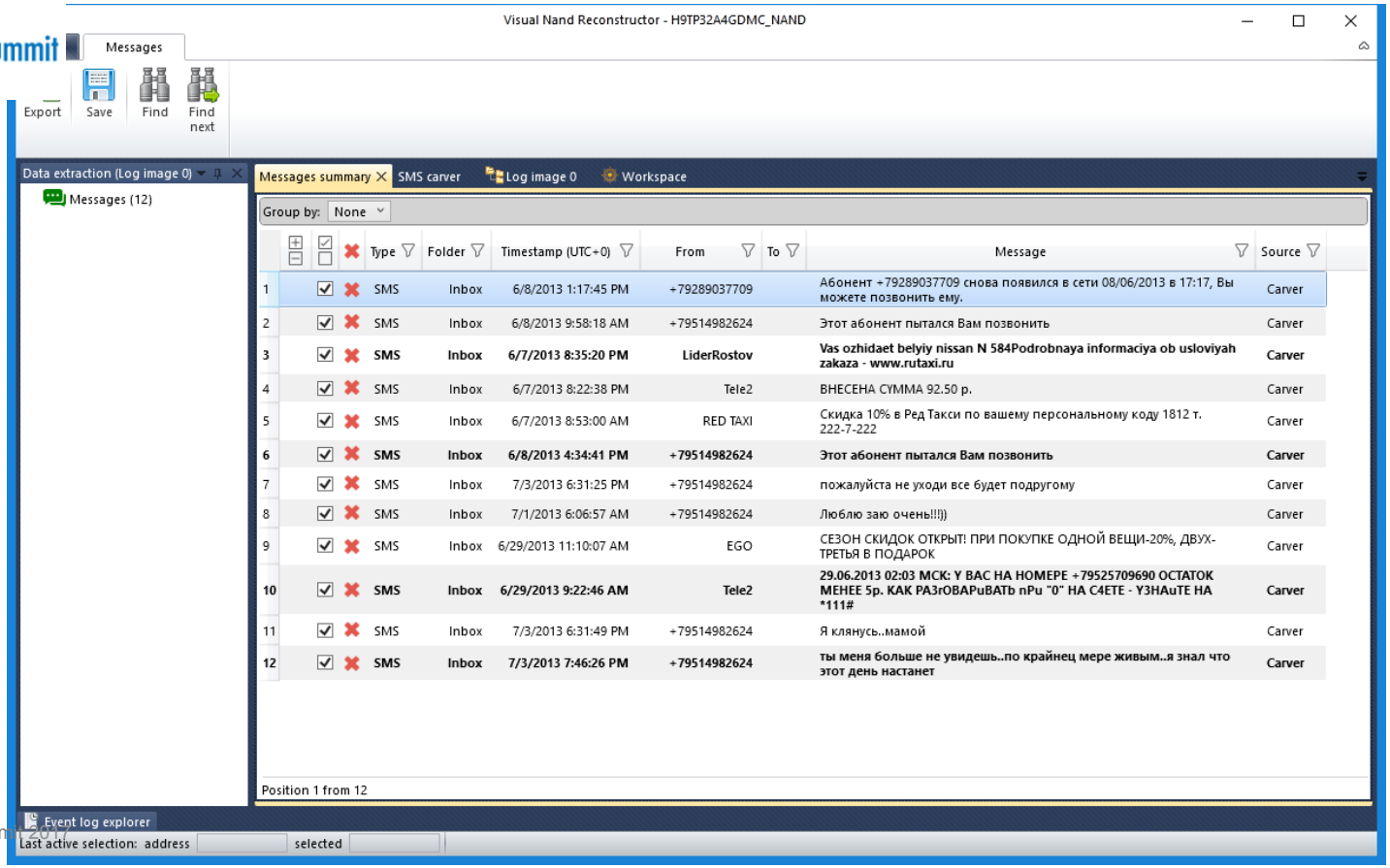
SCRAMBLING


CONTROLLER
DATA
0xBEEFBEEFBEEF
XOR
NOISE (RANDOMIZED)
0x3ABC739D830A
LFSR-key
1
0
0
0
1

DATA REMNANTS AFTER DESCRAMBLING



SMS CARVING RESULTS (FROM ERASED EMMC)



SMS RECOVERY FROM 10 SAME SMARTPHONES (NOT ERASED EMMC)

Green blocks (A,C,D,F,H,J) – more SMS were found in NAND memory chip.

Red blocks (B,E,G,I) – less SMS were found in NAND memory chip due to uncorrectable bit errors caused by threshold voltage shifts (eMMC controller handles it). Further research and improvements of results using Read-retry algorithms are required. More information about this issue can be found in paper written by Aya Fukami here:

http://www.pdl.cmu.edu/PDL-FTP/NVM/17dfrwseu.pdf

A

Source	SMS count	Comparison
NAND	116	**283%**
eMMC	41	100%

B

Source	SMS count	Comparison
NAND	2377	99,75%
eMMC	2383	100%

C

Source	SMS count	Comparison
NAND	4866	**103%**
eMMC	4723	100%

D

Source	SMS count	Comparison
NAND	118	**144%**
eMMC	82	100%

E

Source	SMS count	Comparison
NAND	6753	71%
eMMC	9464	100%

F

Source	SMS count	Comparison
NAND	47	**247%**
eMMC	19	100%

G

Source	SMS count	Comparison
NAND	96	74%
eMMC	129	100%

H

Source	SMS count	Comparison
NAND	105	**525%**
eMMC	20	100%

I

Source	SMS count	Comparison
NAND	244	94%
eMMC	260	100%

J

Source	SMS count	Comparison
NAND	1540	**131%**
eMMC	1174	100%

SUMMARY

THE ULTIMATE GOAL OF DIGITAL FORENSICS AND DATA RECOVERY IS TO EXTRACT AS MUCH DATA OUT OF DEVICE AS POSSIBLE. OUR RESEARCH SHOWS THAT CURRENTLY USED METHODS IN MOBILE FORENSICS AND DATA RECOVERY ARE NOT COMPLETE AND THERE ARE STILL SOME CHUNKS OF DATA REMAIN UNANALYSED. DIRECT ACCESS TO NAND MEMORY OF eMMC IS THE ONLY SUFFICIENT WAY TO MAKE SURE THAT ALL THE DATA HAVE BEEN EXTRACTED AND ANALYSED.

CONTACTS

HEADQUARTERS

www.rusolut.com
Polczynska 10,
Warsaw, Poland
+48 537 202 227
info@rusolut.com

my email: sasha@rusolut.com

LOCAL PARTNERS IN USA

www.cprtools.com
2022 Hendry Street
Suite 100
Fort Myers, FL
239.464.DATA (3282)
support@cprtools.com