



# SMS recovery from NAND memory of erased eMMC chip

Sasha Sheremetov – CTO of Rusolut



Flash Memory Summit

## WHY ERASE EMMC CHIP

In this experiment the eMMC was intentionally erased (zeroed 0x00) through standard interface in order to prove/disprove existence of after-erase data remnants beyond 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

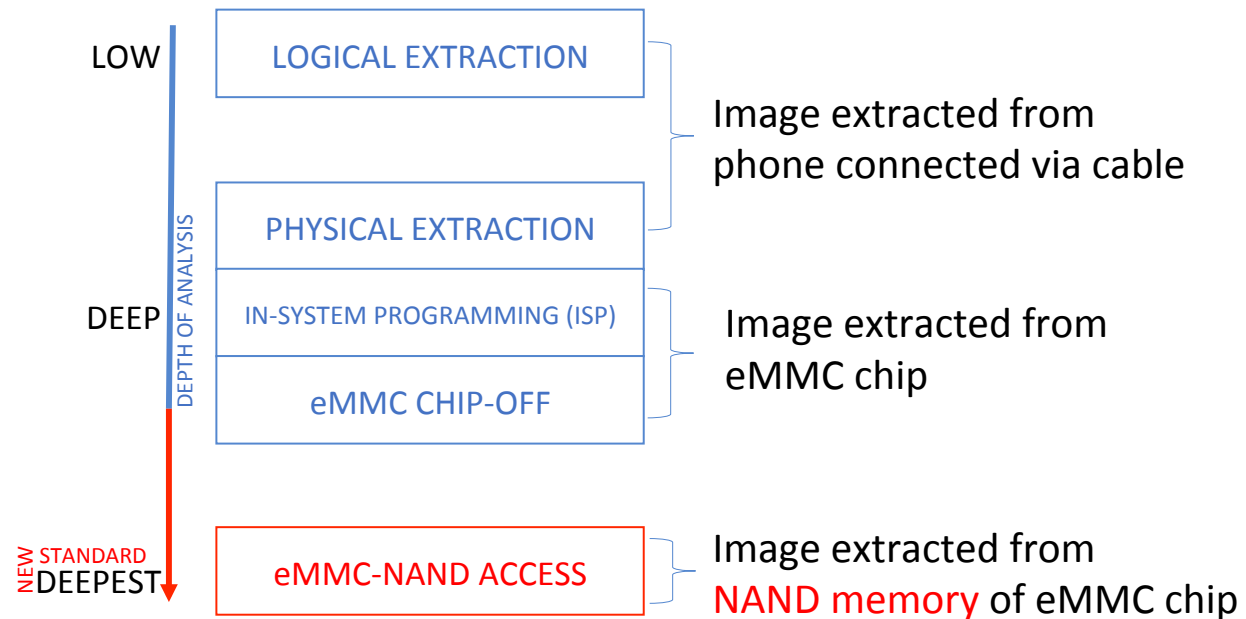
- data recovery of lost or deleted data in case if no desired files found in eMMC
- data recovery via direct access to NAND memory of damaged eMMC (when controller failed to start up and device is not reacting on commands)

### DIGITAL FORENSICS

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



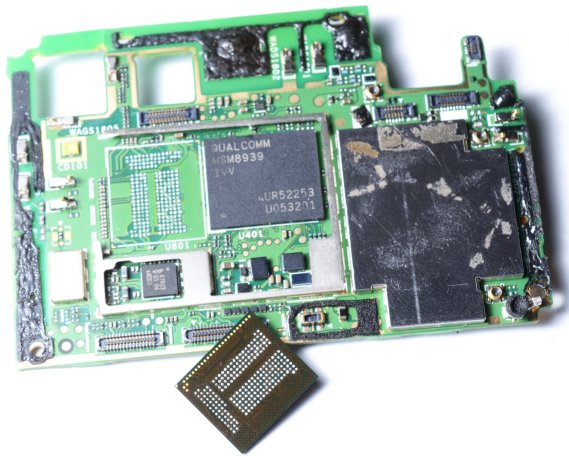
## DIFFERENT WAYS OF DATA EXTRACTION AND ANALYSIS FROM ANDROID SMARTPHONES





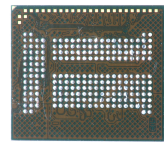
## CLASSIC CHIP-OFF AND DATA EXTRACTION FROM eMMC CHIP

### PHYSICAL IMAGE EXTRACTION

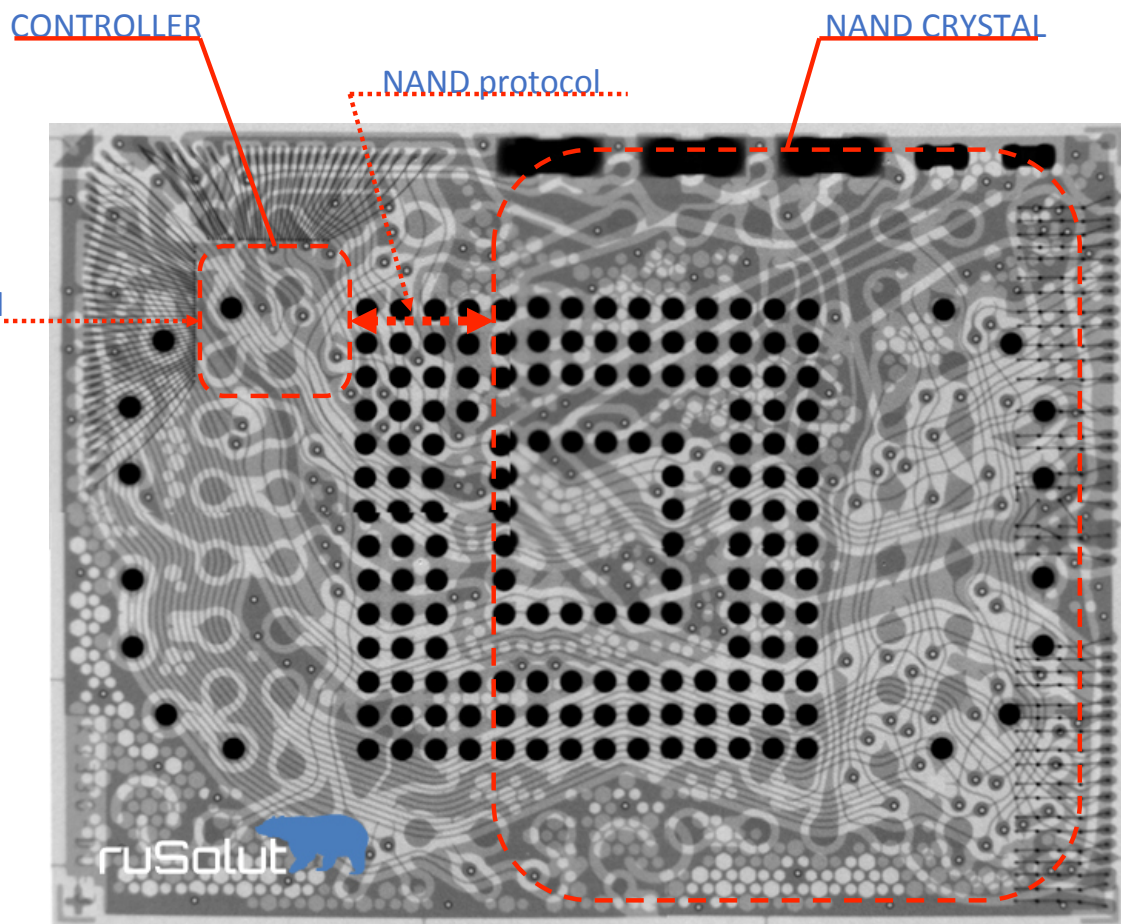


UNSOLDERING

### CLEANING



# eMMC CHIP STRUCTURE THROUGH XRAY

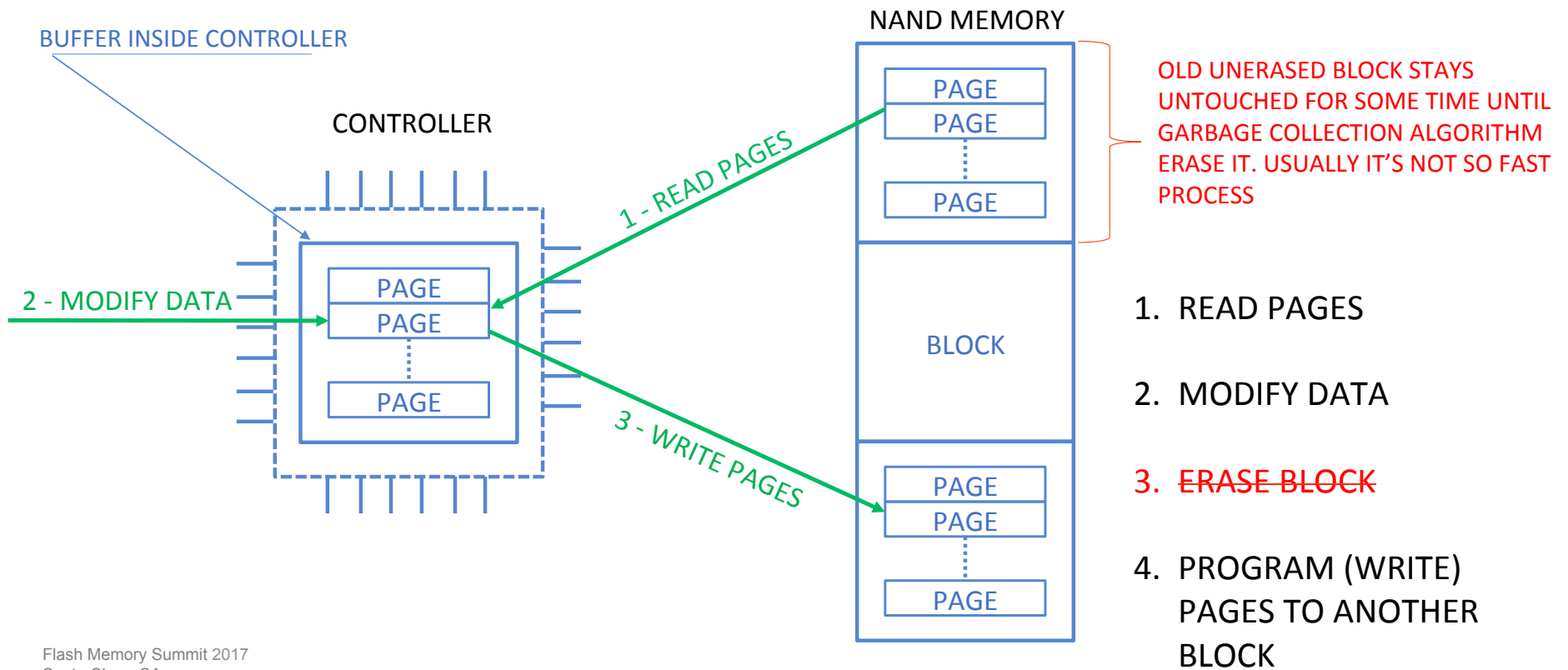


ruSolut

eMMC = RAW NAND + CONTROLLER



## HOW DATA MODIFICATION PROCESS WORKS IN NAND MEMORY





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

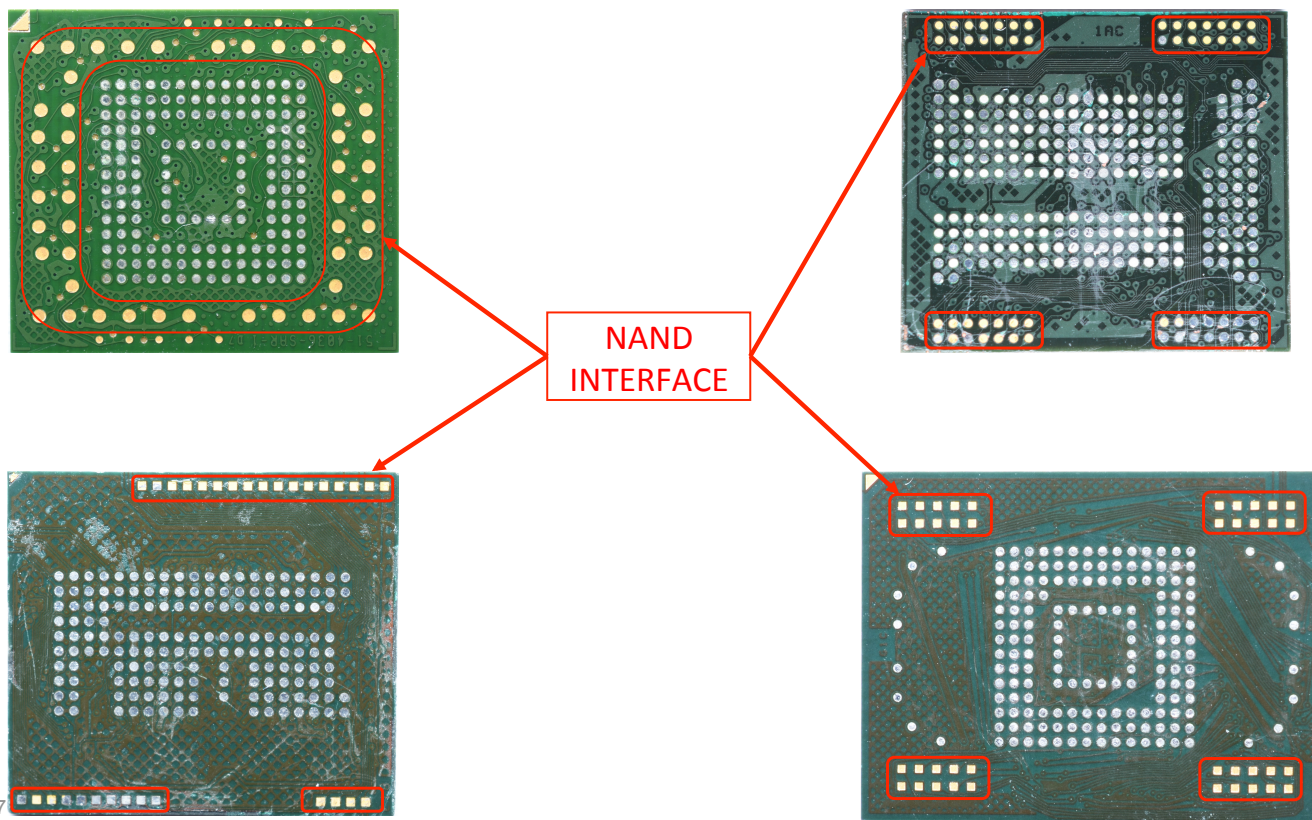
TO MAKE THINGS WORSE LET'S **ERASE** EMMC CHIP!



## 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



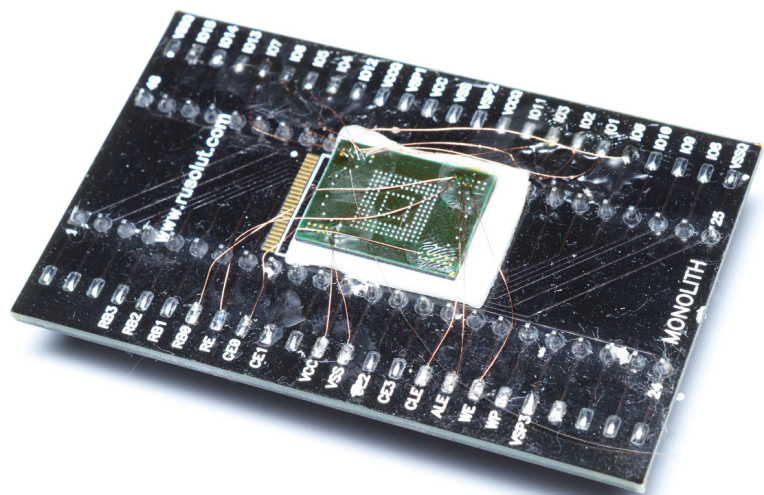




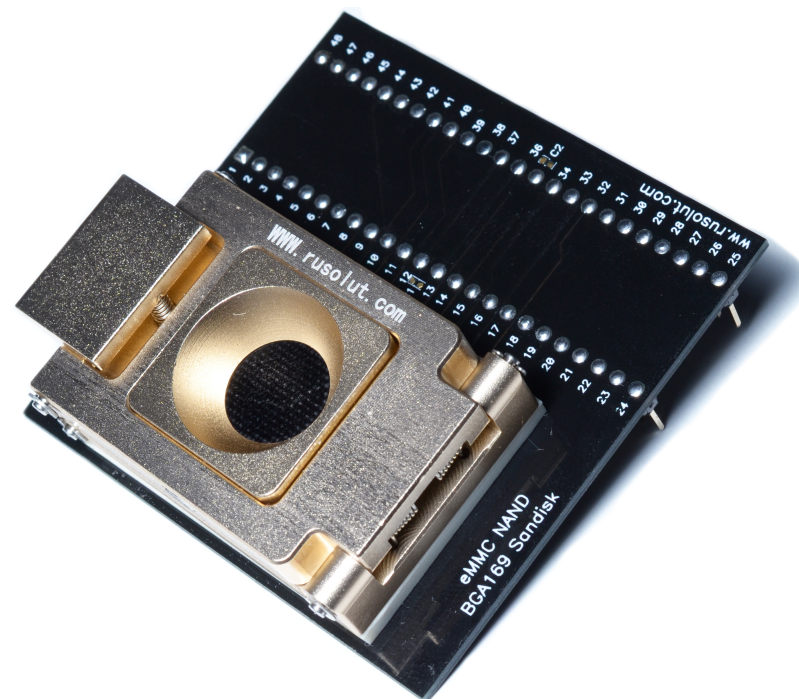
Flash Memory Summit

## eMMC CHIP ON ADAPTER CONNECTED VIA NAND PROTOCOL

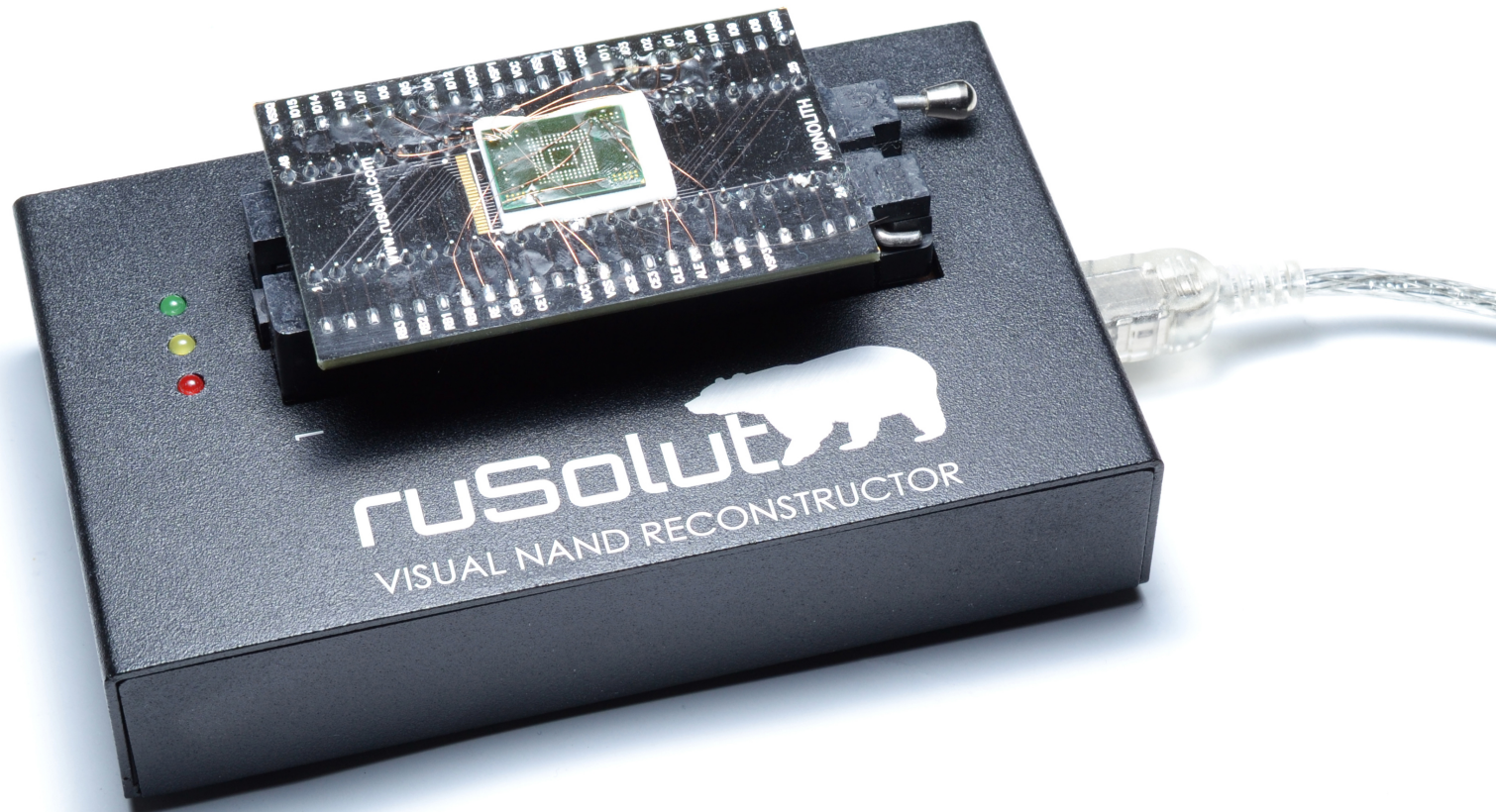
COMPLICATED WAY



EASY WAY



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



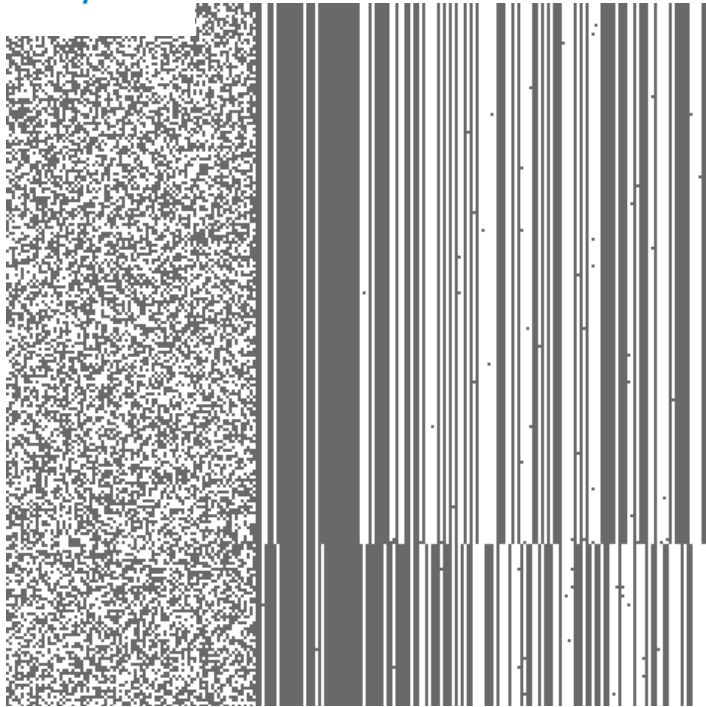




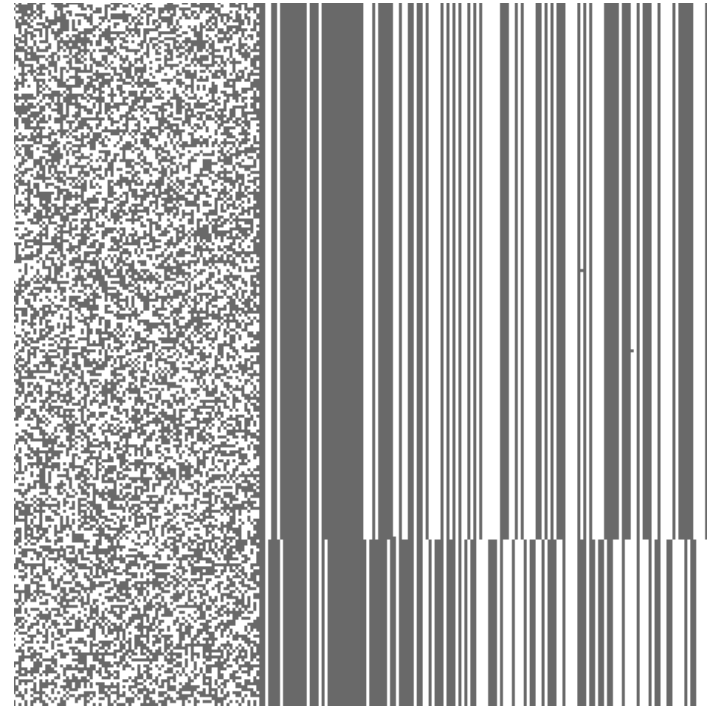
Flash Memory Summit

## BIT ERRORS AND ECC CORRECTION

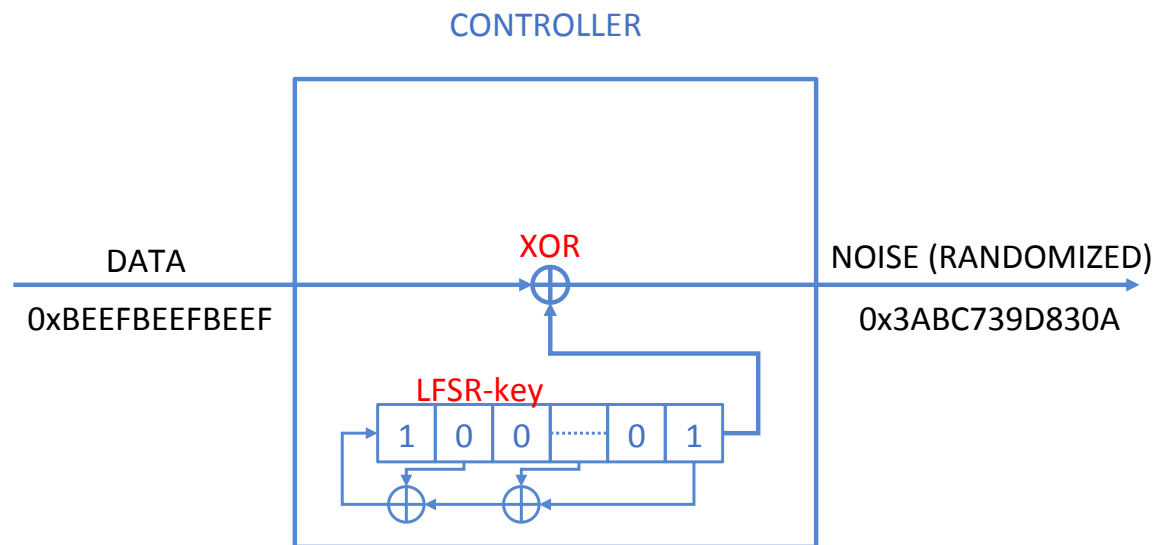
BEFORE ECC



AFTER ECC



## SCRAMBLING





Flash Memory Summit

# DATA REMNANTS AFTER DESCRAMBLING

The screenshot shows the Visual NAND Reconstructor interface. The main workspace displays hex data on the left and its corresponding ASCII output on the right. The hex data is organized into columns labeled 00 through 0F. The ASCII output shows various characters, including symbols like asterisks, dots, and question marks, along with some recognizable strings like 'URR', 'P', and 'CFCFPeC'. The status bar at the bottom indicates the current address and selection.

Address	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	ASCII
0044C4D680	2A	1D	00	25	05	02	01	08	29	01	00	11	00	00	25	00	*.%......).%. .....+7
0044C4D690	00	00	08	00	00	00	00	00	00	00	01	08	02	02	2B	37	9613217706.?(%a[ ...P&P*%P*%wC&C
0044C4D6A0	39	36	31	33	32	31	37	37	30	36	01	3F	7B	5E	61	7B	U.RUP P&cFCFPeCU ...sUs%.....)
0044C4D6B0	01	0E	02	D0	9D	D0	B0	D1	82	D0	B0	D0	BB	D1	8C	D1	.....+7951498262
0044C4D6C0	8F	02	52	55	D0	A0	D0	BE	D1	81	D1	81	D0	B8	D1	8F	4.?[ ]_k-.P PaPjP *C+PeP*.RUP PaCjP
0044C4D6D0	04	0B	26	1B	9F	53	8E	29	1D	00	25	05	01	01	08	29	CfPeCU...US%(... %.....).%.+7951
0044C4D6E0	01	00	11	00	00	25	00	00	00	08	00	00	00	00	00	00	.....+7951498262
0044C4D6F0	00	01	08	02	02	2B	37	39	35	31	34	39	38	32	36	32	4.?[ ]_k-.P PaPjP *C+PeP*.RUP PaCjP
0044C4D700	34	01	3F	7B	5D	5F	9D	2D	02	D0	A0	D0	BE	D0	BC	D0	CfPeCU...US%(... %.....).%.+7951
0044C4D710	B0	D1	87	D0	BA	D0	B0	02	52	55	D0	A0	D0	BE	D1	81	.....+7951498262
0044C4D720	D1	81	D0	B8	D1	8F	04	0A	1E	19	8F	53	8E	28	1D	00	jP*C+PeP*.RUP Pa CfCfPeCU...U7% U....UT%..\$...... ).....+7951498262
0044C4D730	25	05	01	01	08	29	01	00	11	00	00	25	05	00	00	08	24.?(QMs.H.P PaP jP*C+PeP*.RUP Pa CfCfPeCU...U7% U....UT%..\$...... ).....+7951498262
0044C4D740	00	00	00	00	00	00	00	01	08	02	02	2B	37	39	35	31	.....+7951498262
0044C4D750	34	39	38	32	36	32	34	01	3F	7B	55	9B	0E	11	02	D0	.....+7951498262
0044C4D760	A0	D0	BE	D0	BC	D0	B0	D1	87	D0	BA	D0	B0	02	52	55	PaPjP*C+PeP*.RU P PaCFCFPeC*.... URR'.....).%. %.+7951498262.?( U<T.P PaPjP*C+Pe P*.RUP PaCFCFPeC U....UT%..\$...... ).....+7951498262
0044C4D770	D0	A0	D0	BE	D1	81	D1	81	D0	B8	D1	8F	04	0A	1E	19	.....+7951498262
0044C4D780	8F	52	8E	27	1D	00	25	05	08	01	08	29	01	00	11	00	.....+7951498262
0044C4D790	00	25	00	00	00	08	00	00	00	00	00	00	00	00	01	08	24.?(QMs.H.P PaP jP*C+PeP*.RUP Pa CfCfPeCU...U7% U....UT%..\$...... ).....+7951498262
0044C4D7A0	02	2B	37	39	35	31	34	39	38	32	36	32	34	01	3F	7B	.....+7951498262
0044C4D7B0	55	3C	D2	02	D0	A0	D0	BE	D0	BC	D0	B0	D1	87	D0	BA	.....+7951498262
0044C4D7C0	D0	B0	02	52	55	D0	A0	D0	BE	D1	81	D1	81	D0	B8	D1	.....+7951498262
0044C4D7D0	8F	04	0A	1E	19	8F	54	8E	26	1D	00	25	05	02	01	08	.....+7951498262
0044C4D7E0	29	01	00	11	00	00	25	00	00	00	00	00	00	00	00	00	.....+7951498262
0044C4D7F0	00	00	01	08	02	02	2B	37	39	35	31	34	39	38	32	36	.....+7951498262
0044C4D800	32	34	01	3F	7B	51	CC	9A	00	CD	02	D0	A0	D0	BE	D0	.....+7951498262
0044C4D810	BC	D0	B0	D1	87	D0	BA	D0	B0	02	52	55	D0	A0	D0	BE	.....+7951498262
0044C4D820	D1	81	D1	81	D0	B8	D1	8F	04	0A	1E	19	8F	3F	8E	25	.....+7951498262
0044C4D830	1D	00	25	05	01	09	08	00	08	00	11	00	00	25	00	00	.....+7951498262
0044C4D840	00	08	00	00	00	00	00	00	00	01	08	00	00	2B	37	39	.....+7951498262
0044C4D850	30	36	33	30	37	35	33	39	39	01	3F	7B	51	31	61	11	.....+7951498262
0044C4D860	52	55	D0	A0	D0	BE	D1	81	D1	81	D0	B8	D1	8F	04	54	.....+7951498262
0044C4D870	8E	24	1D	00	25	05	02	01	08	29	01	00	11	00	00	25	.....+7951498262
0044C4D880	00	00	00	08	00	00	00	00	00	00	00	01	08	02	02	2B	.....+7951498262
0044C4D890	37	39	35	31	34	39	38	32	36	32	34	01	3F	7B	4E	92	.....+7951498262
0044C4D8A0	8C	00	BA	02	D0	A0	D0	BE	D0	BC	D0	B0	D1	87	D0	BA	.....+7951498262
0044C4D8B0	D0	B0	02	52	55	D0	A0	D0	BE	D1	81	D1	81	D0	B8	D1	.....+7951498262
0044C4D8C0	8F	04	0A	1E	19	8F	53	8E	23	1D	00	25	05	01	01	08	.....+7951498262
0044C4D8D0	29	01	00	11	00	00	25	00	00	00	00	00	00	00	00	00	.....+7951498262

Flash Memory Summit 20  
Santa Clara, CA



Flash Memory Summit

## SMS CARVING RESULTS (FROM ERASED EMMC)

Visual Nand Reconstructor - H9TP32A4GDMC\_NAND

Messages

Export Save Find Find next

Data extraction (Log image 0) Messages summary SMS carver Log Image 0 Workspace

Messages (12)

Group by: None

	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Type	Folder	Timestamp (UTC-0)	From	To	Message	Source
1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	SMS	Inbox	6/8/2013 1:17:45 PM	+79289037709		Абонент +79289037709 снова появился в сети 08/06/2013 в 17:17, Вы можете позвонить ему.	Carver
2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	SMS	Inbox	6/8/2013 9:58:18 AM	+79514982624		Этот абонент пытался Вам позвонить	Carver
3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	SMS	Inbox	6/7/2013 8:35:20 PM	LiderRostov		Vas ozhidaet belyiy nissan N 584Podrobnaya informaciya ob usloviyah zakaza - www.rutaxi.ru	Carver
4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	SMS	Inbox	6/7/2013 8:22:38 PM	Tele2		ВНЕСЕНА СУММА 92.50 р.	Carver
5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	SMS	Inbox	6/7/2013 8:53:00 AM	RED TAXI		Скидка 10% в Ред Такси по вашему персональному коду 1812 т. 222-7-222	Carver
6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	SMS	Inbox	6/8/2013 4:34:41 PM	+79514982624		Этот абонент пытался Вам позвонить	Carver
7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	SMS	Inbox	7/3/2013 6:31:25 PM	+79514982624		пожалуйста не уходи все будет по другому	Carver
8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	SMS	Inbox	7/1/2013 6:06:57 AM	+79514982624		Люблю заю очень!!!!)	Carver
9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	SMS	Inbox	6/29/2013 11:10:07 AM	EGO		СЕЗОН СКИДОК ОТКРЫТ: ПРИ ПОКУПКЕ ОДНОЙ ВЕЩИ-20%, ДВУХ- ТРЕТЬЯ В ПОДАРОК	Carver
10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	SMS	Inbox	6/29/2013 9:22:46 AM	Tele2		29.06.2013 02:03 МСК: У ВАС НА НОМЕРЕ +79525709690 ОСТАТОК МЕНЕЕ 5р. КАК РАЗГОВАРИВАТЬ нRu "0" НА СЧЕТЕ - УЗНАУТЕ НА *111#	Carver
11	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	SMS	Inbox	7/3/2013 6:31:49 PM	+79514982624		Я кланюсь..мамой	Carver
12	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	SMS	Inbox	7/3/2013 7:46:26 PM	+79514982624		ты меня больше не увидешь..по крайнее мере живым..я знал что этот день настанет	Carver

Position 1 from 12

Event log explorer  
Last active selection: address selected

Flash Memory Summit 2017  
Santa Clara, CA



## 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%

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

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

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

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

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

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

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

E		
Source	SMS count	Comparison
NAND	6753	71%
eMMC	9464	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](http://www.rusolut.com)  
Polczynska 10,  
Warsaw, Poland  
+48 537 202 227  
[info@rusolut.com](mailto:info@rusolut.com)

my email: [sasha@rusolut.com](mailto:sasha@rusolut.com)

### LOCAL PARTNERS IN USA



[www.cprtools.com](http://www.cprtools.com)  
2022 Hendry Street  
Suite 100  
Fort Myers, FL  
239.464.DATA (3282)  
[support@cprtools.com](mailto:support@cprtools.com)