eMMC CHIPS. DATA RECOVERY BEYOND CONTROLLER

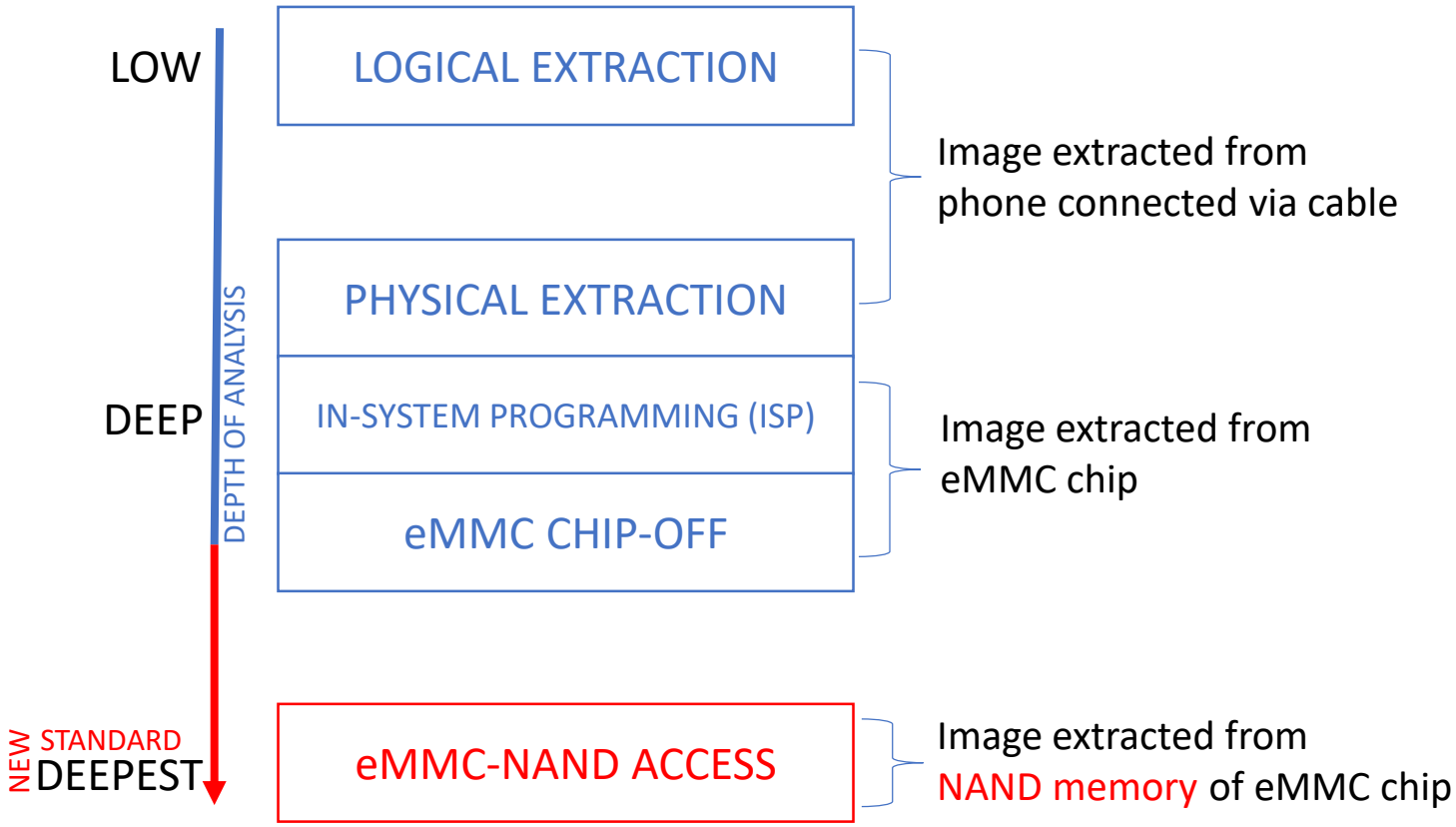
Rusolut

APPLICATIONS OF EMMC CHIPS

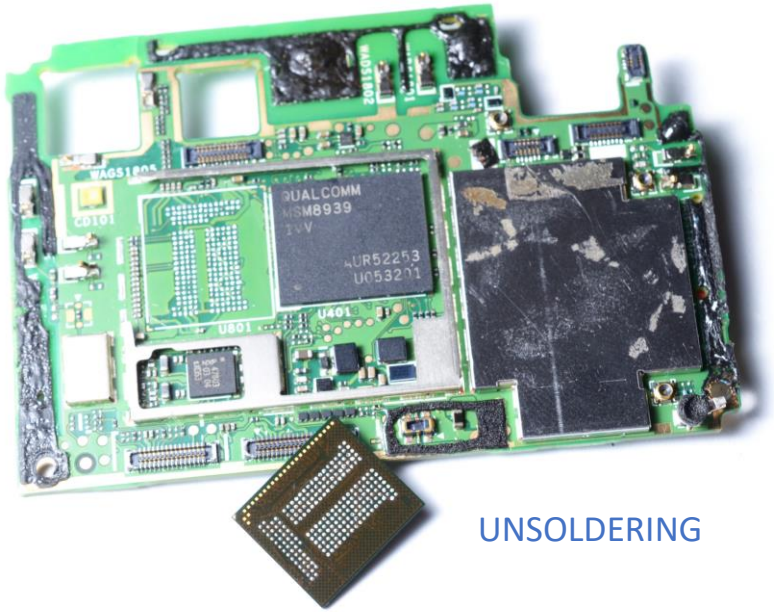
- SMARTPHONES
- TABLETS
- LAPTOPS
- VOICE RECORDERS
- CAMERAS
- MULTIMEDIA PLAYERS
- TV DECODERS
- INTERNET OF THINGS

…AND MUCH MORE…

DIFFERENT WAYS OF IMAGE EXTRACTION FROM DEVICES BASED ON EMMC CHIPS

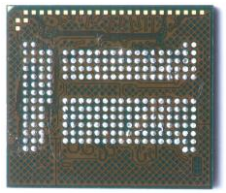


CLASSIC CHIP-OFF AND DATA EXTRACTION FROM eMMC CHIP



UNSOLDERING

CLEANING

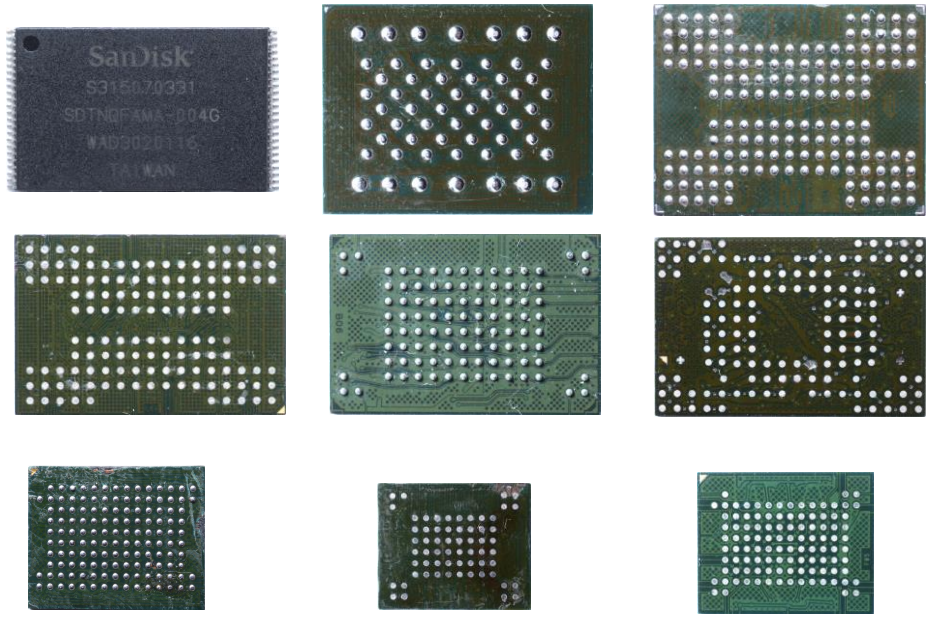


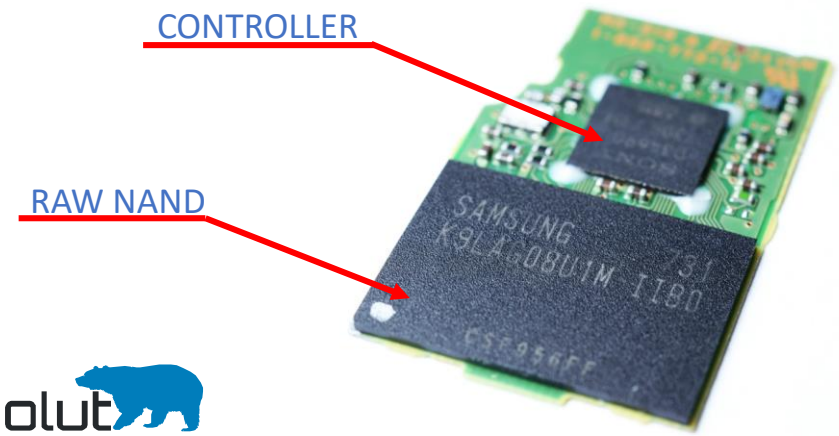
PHYSICAL IMAGE EXTRACTION

ruSolut

FLASH MEMORY CHIPS

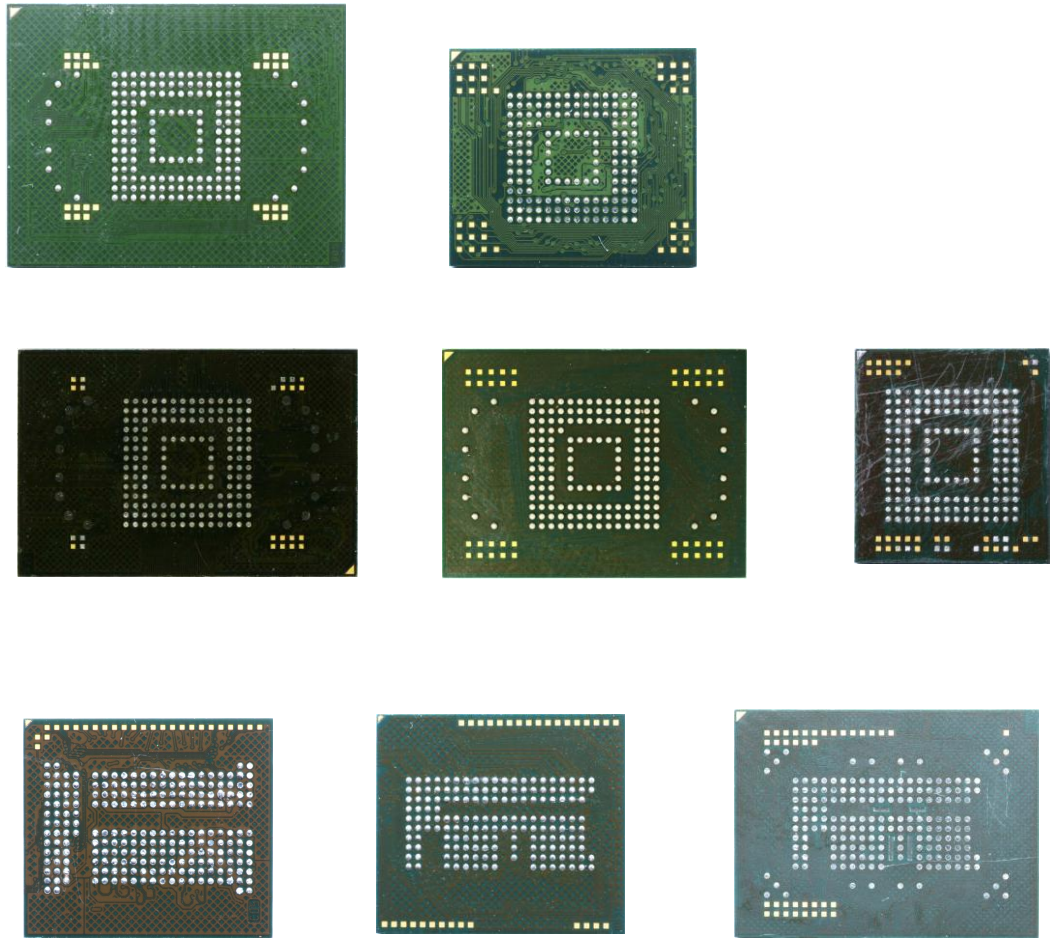
NAND





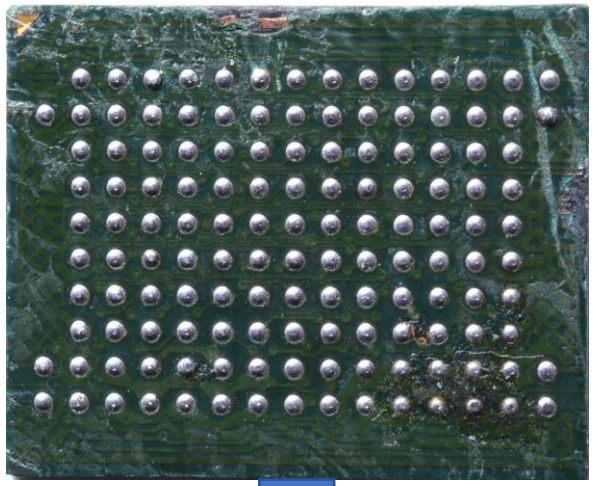
eMMC

AREA OF INTEREST



EMMC vs RAW NAND CHIP-OFF DATA RECOVERY

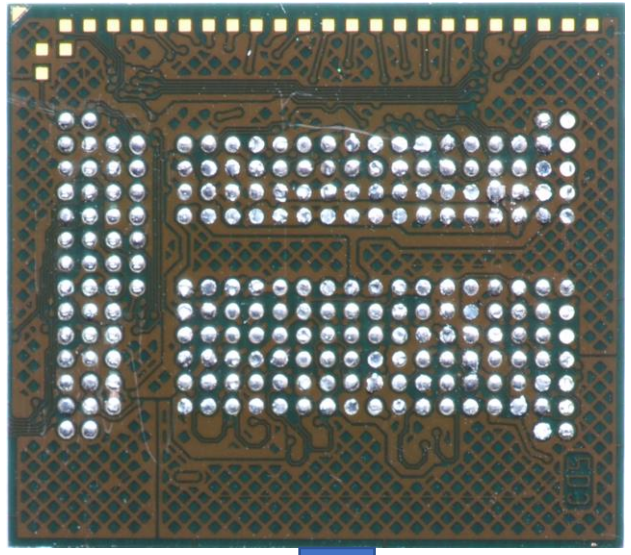
NAND



READ

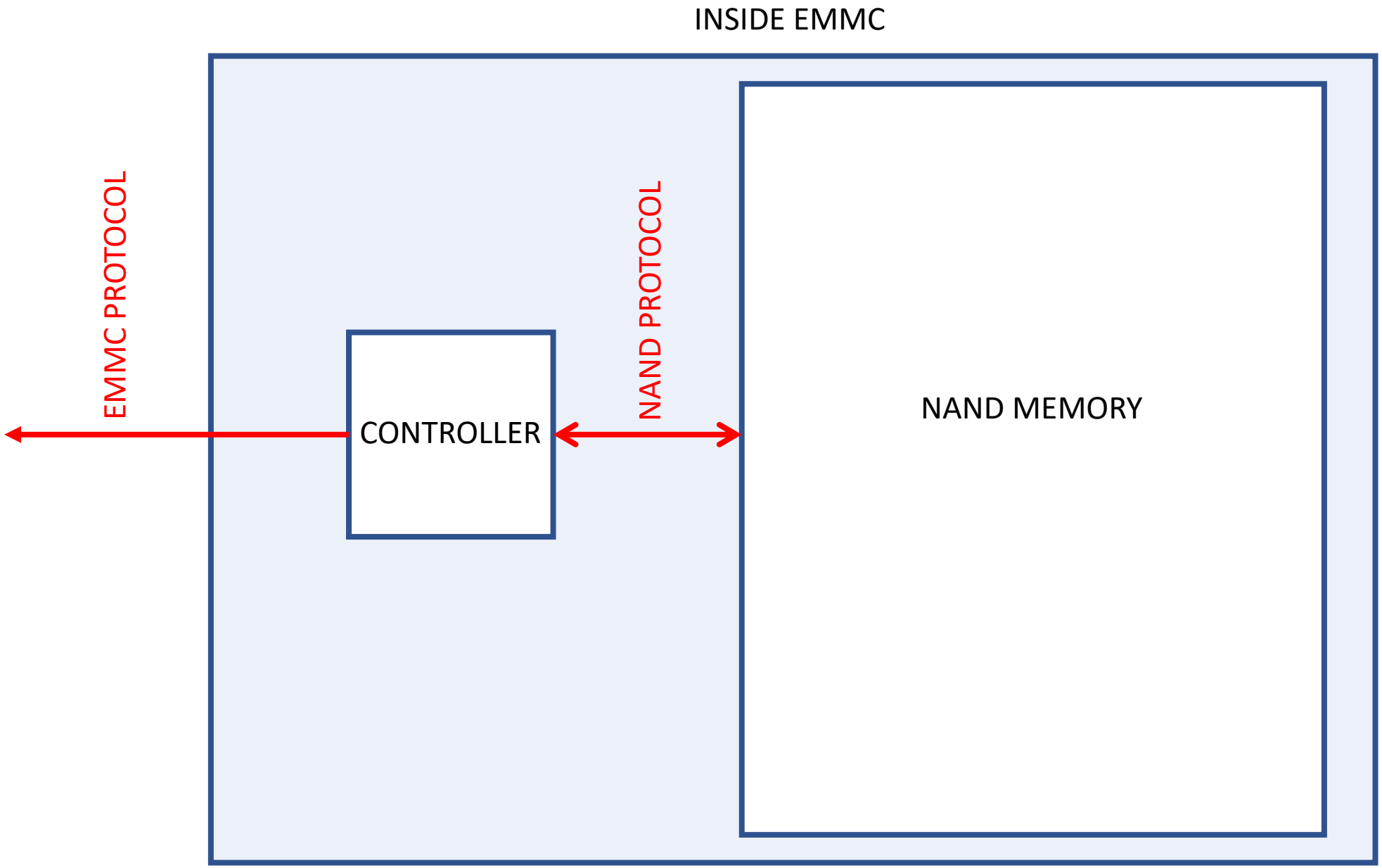
NAND protocol

eMMC/eMCP

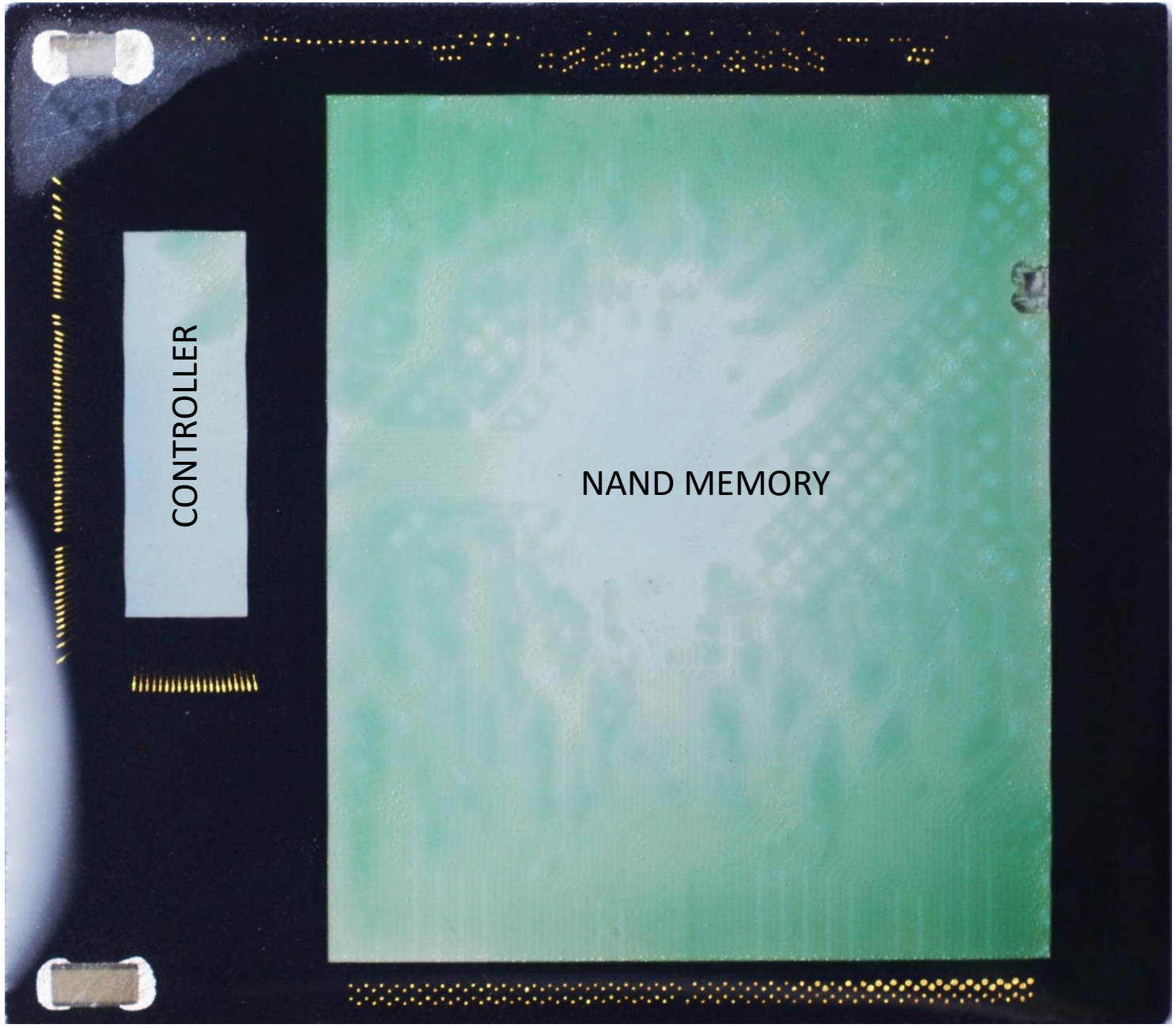


eMMC protocol

READ


INSIDE EMMC
EMMC PROTOCOL
NAND PROTOCOL
CONTROLLER
NAND MEMORY

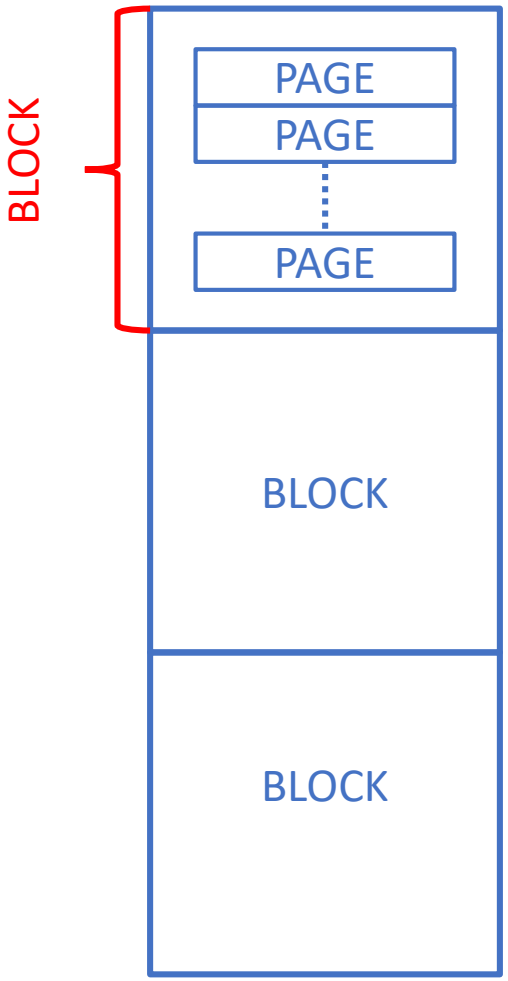
EMMC CHIP STRUCTURE



WHY CARE ABOUT GETTING DATA VIA NAND FROM EMMC?

- DAMAGED EMMC CHIPS
- FACTORY RESET
- ERASED DATA RECOVERY

NAND MEMORY ADDRESSING AND R/W OPERATIONS



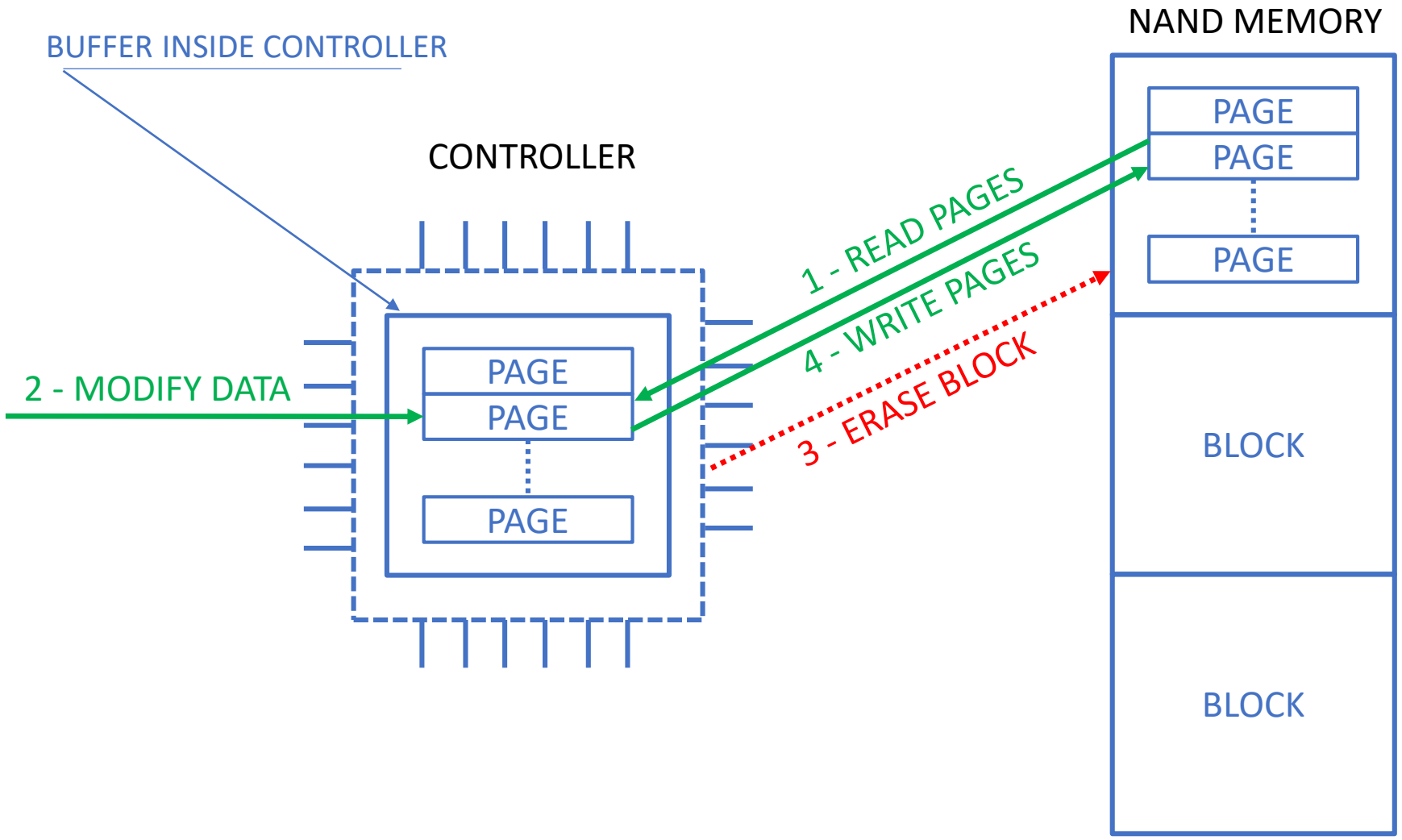
- READ PAGE
- PROGRAM (WRITE) PAGE
- ERASE BLOCK

PAGE IS A SMALLEST R/W UNIT

BLOCK IS A SMALLEST ERASE UNIT

PAGE SIZE = 0,5 - 16Kb
BLOCK SIZE = 128Kb – 4Mb

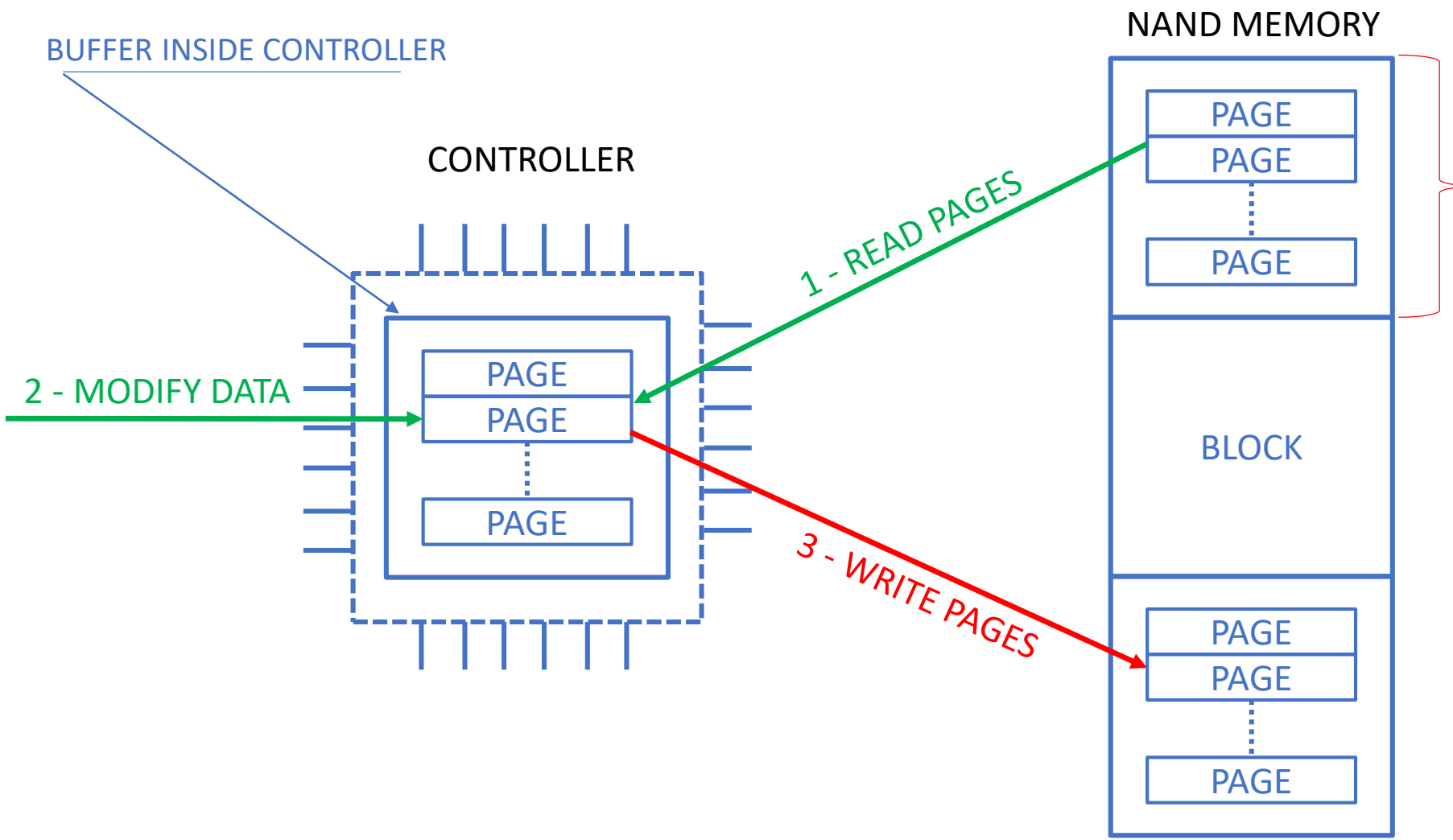
HOW DATA MODIFICATION PROCESS IS SUPPOSED TO WORK IN NAND MEMORY



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

ruSolut

HOW DATA MODIFICATION PROCESS ACTUALLY 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. PROGRAM (WRITE) PAGES

ruSolut

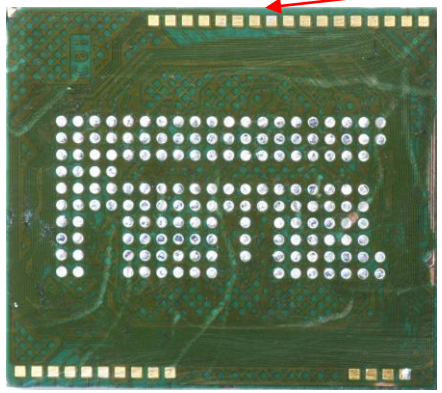
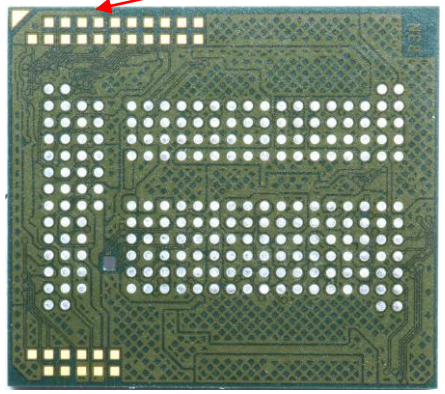
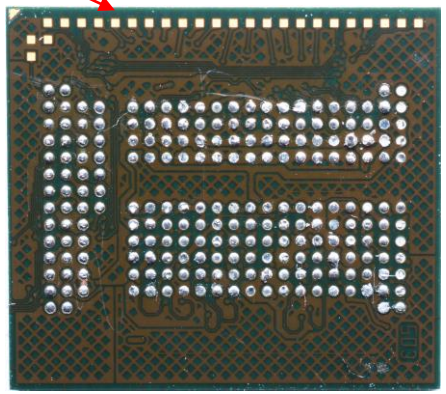
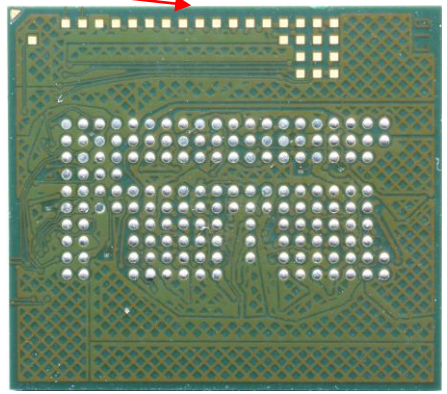
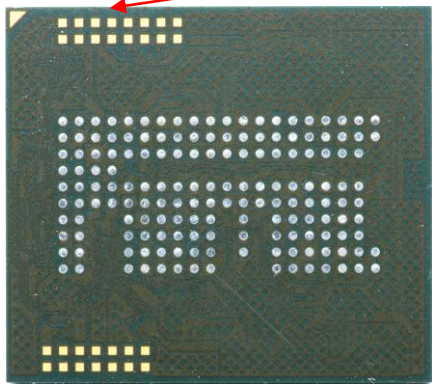
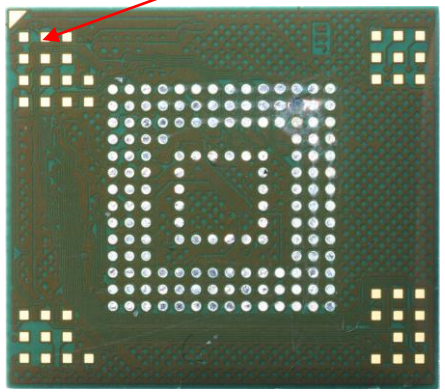
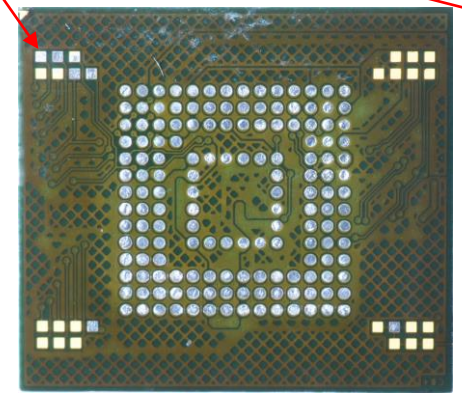
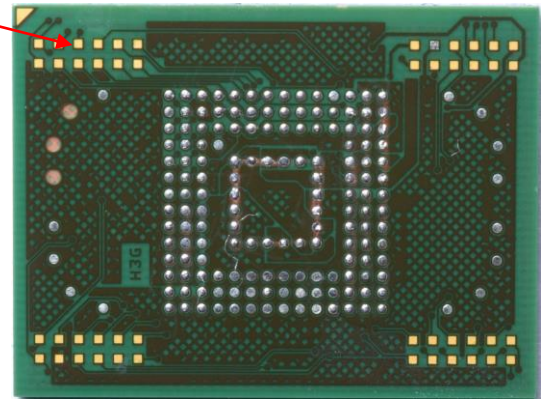
LET’S TRY TO EXTRACT SOME DELETED SMS FROM THOSE “OVERWRITTEN” GARBAGE BLOCKS OF eMMC MEMORY VIA NAND INTERFACE

TO MAKE THINGS WORSE LET’S ERASE EMMC CHIP!

THERE ARE SEVERAL STEPS…

- 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)

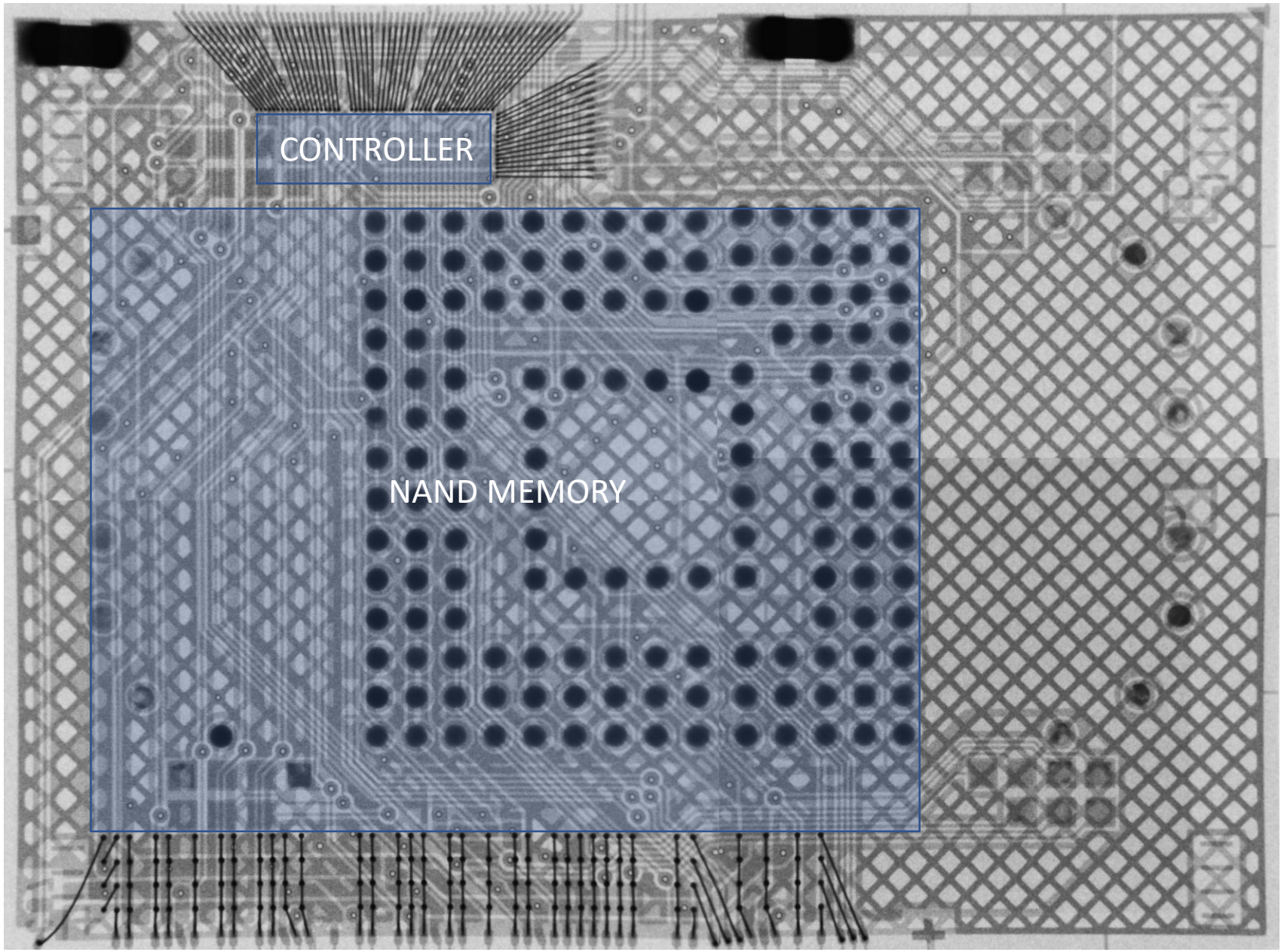
TECHNOLOGICAL PADS - NAND INTERFACE

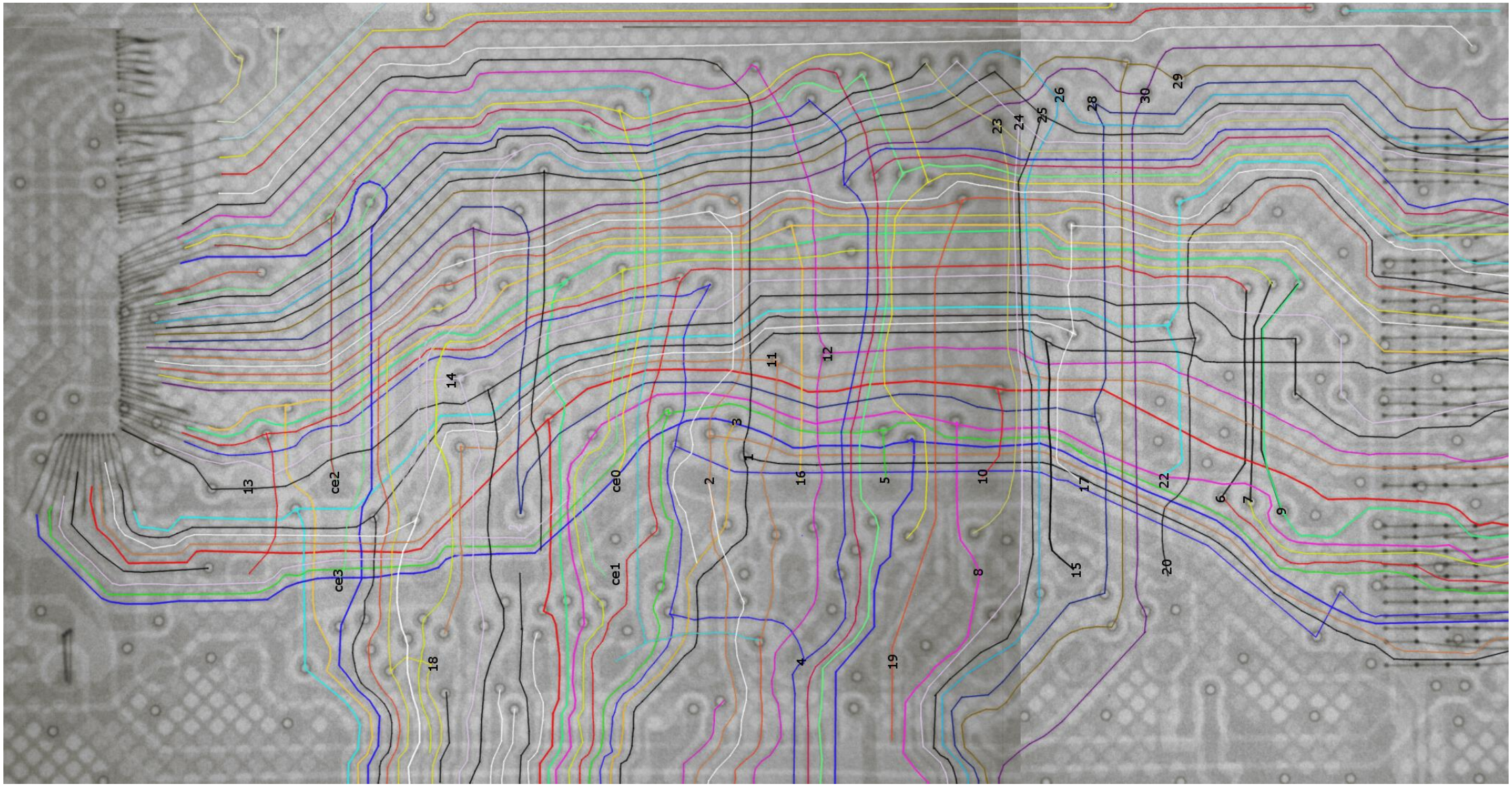
NAND PINOUT ANALYSIS

- XRAY PCB LAYOUT ANALYSIS WITH FURTHER WIRE BONDING ANALYSIS OF NAND AND CONTROLLER
- NAND AND CONTROLLER PINOUT ANALYSIS THROUGH PCB LAYER REMOVAL
- CLASSIC “MAN IN THE MIDDLE ATTACK” USING LOGIC ANALYZER CONNECTED BETWEEN CONROLLER AND NAND MEMORY

EMMC THROUGH XRAY

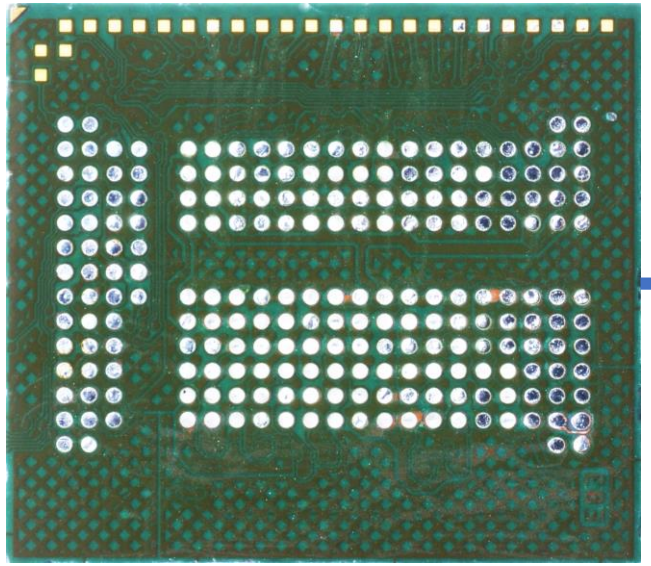


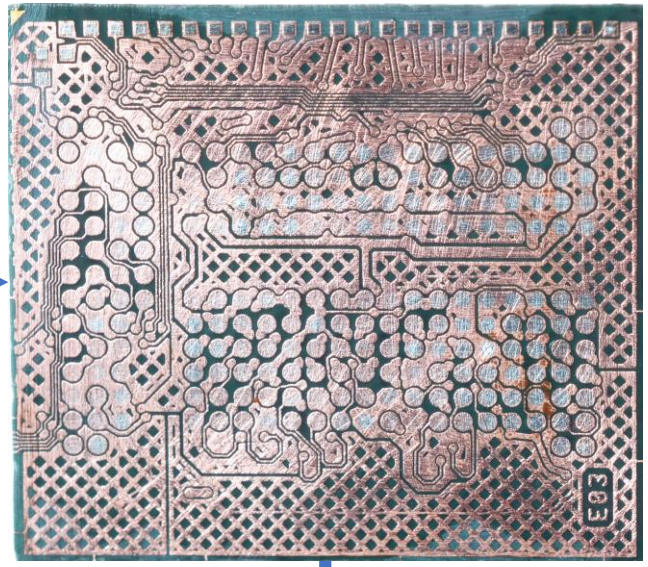
NAND PINOUT ANALYSIS. XRAY

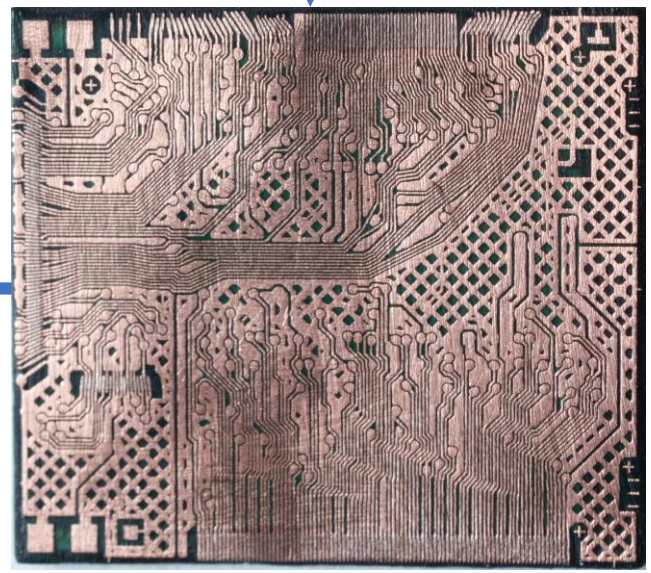


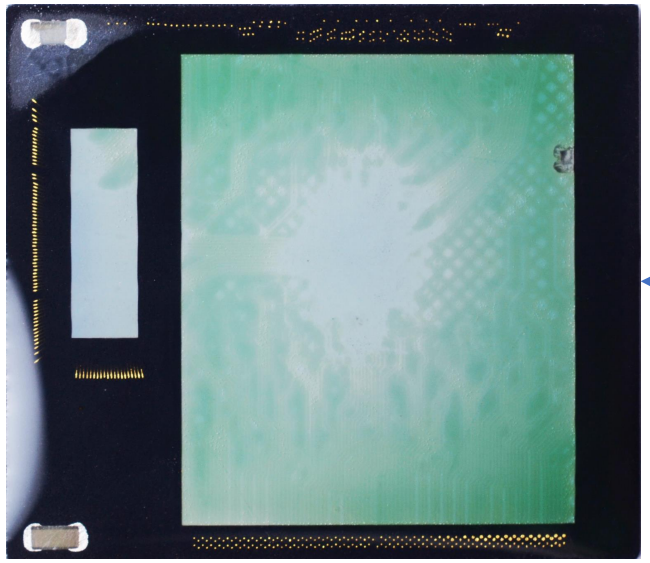
ruSolut

DELAYERED EMMC CHIP

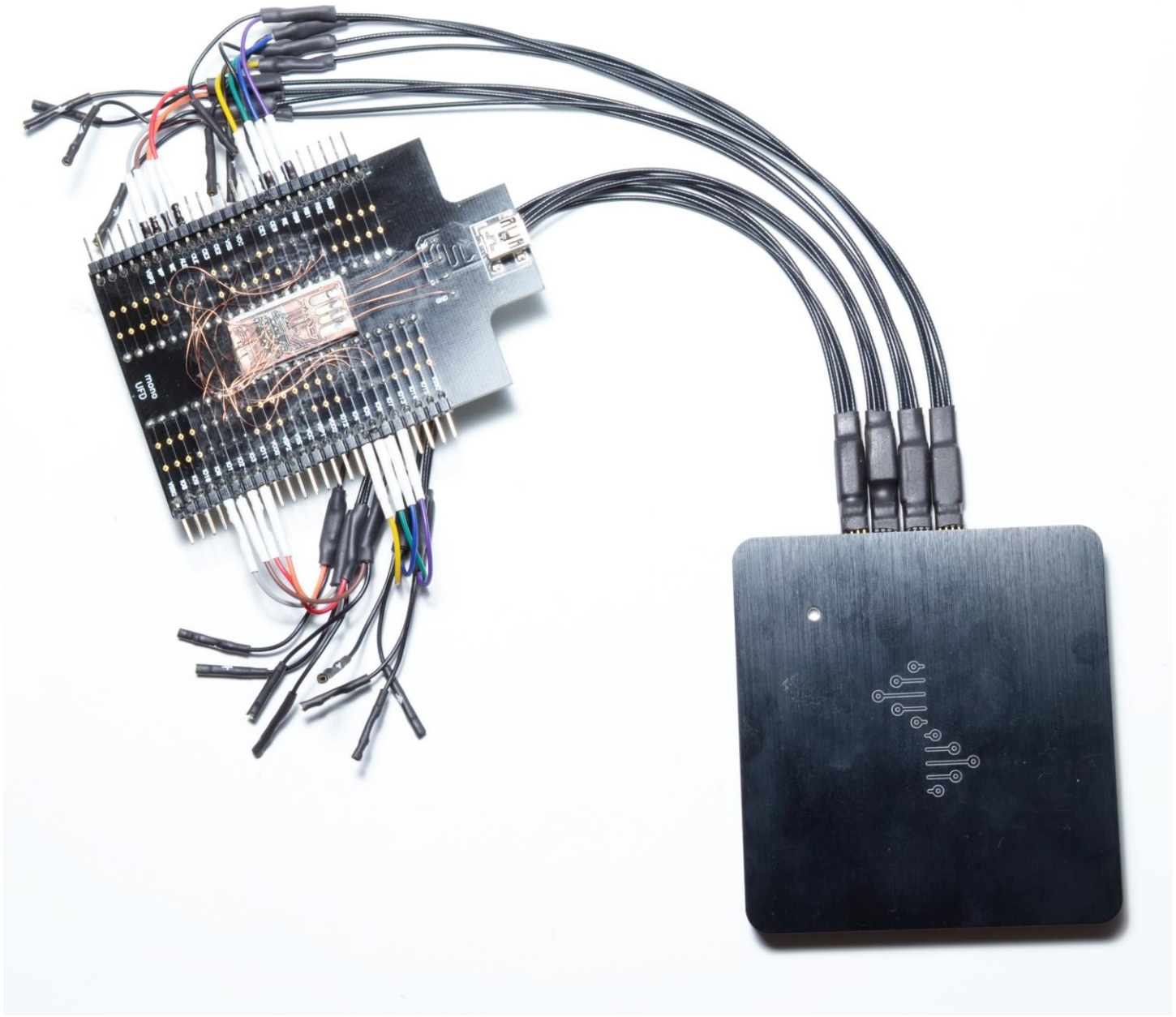




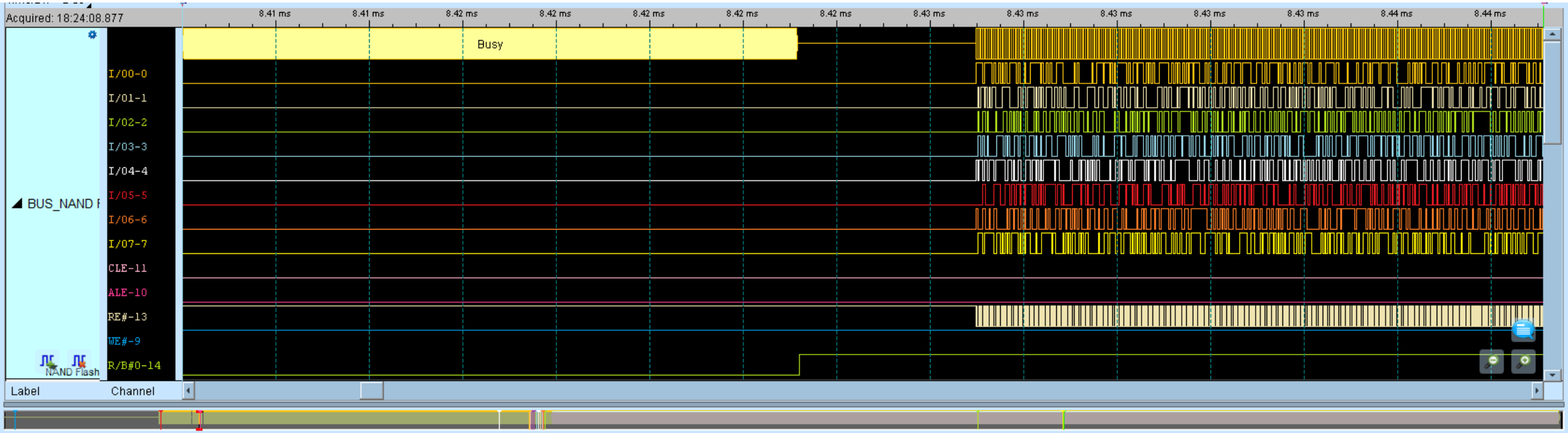




NAND PINOUT ANALYSIS. LOGIC ANALYZER



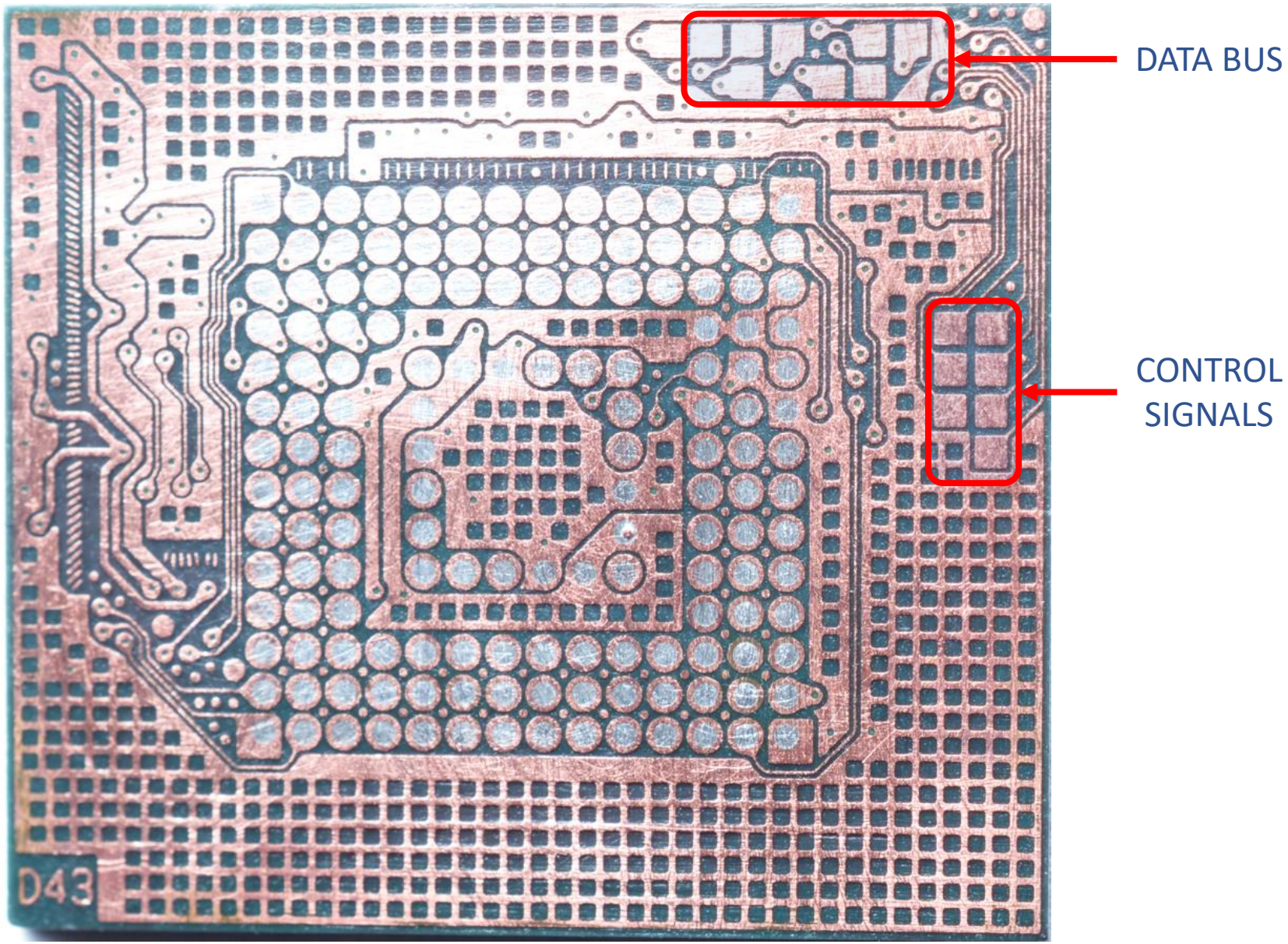
NAND PINOUT ANALYSIS. LOGIC ANALYZER



CH-00 CH-01 | Bus | BUS_NAND Flash(NAND Flash) | Search All Field

	Sample	Command	Row Address(h)	Column / Feature Address(h)	D0	D1	D2	D3	D4	D5	D6	D7	ASCII(D0-D7)
98	8.34249ms	READ #2(30)	000412	0000	51	8F	99	93	6E	F5	93	8D	Q...n...
99	8.81214ms	RESET(FF)											
100	8.82578ms	READ #1(00)	000600	0000									
101	8.83052ms	READ #2(30)	000600	0000	3B	0A	F9	AA	06	43	AB	6D	;....C.m
102	9.35098ms	RESET(FF)											
103	9.365925ms	READ #1(00)	000601	0000									
104	9.370675ms	READ #2(30)	000601	0000	41	76	9E	C9	19	A9	70	04	Av....p.
105	9.51533ms	READ #1(00)	00040A	0000									
106	9.516805ms	READ #2(30)	00040A	0000	4C	C1	0A	03	D3	C4	D5	A7	L.....
107	9.965015ms	READ #1(00)	000412	0000									
108	9.966495ms	READ #2(30)	000412	0000	51	8F	99	93	6E	F5	93	8D	Q...n...
109	10.4473ms	READ #1(00)	000413	0000									
110	10.448715ms	READ #2(30)	000413	0000	01	DF	7E	1B	07	8F	2D	F7	..~...-.
111	10.92589ms	RESET(FF)											
112	10.940395ms	RESET(FF)	FFFFFF	FFFF									
113	10.94419ms	RESET(FF)			00	00	00	00	00	00	00	00	....
114	11.04347ms	RESET(FF)											
115	11.05801ms	RESET(FF)	FFFFFF	FFFF									
116	11.0618ms	RESET(FF)			00	00	00	00	00	00	00	00	....
117	11.111555ms	RESET(FF)											

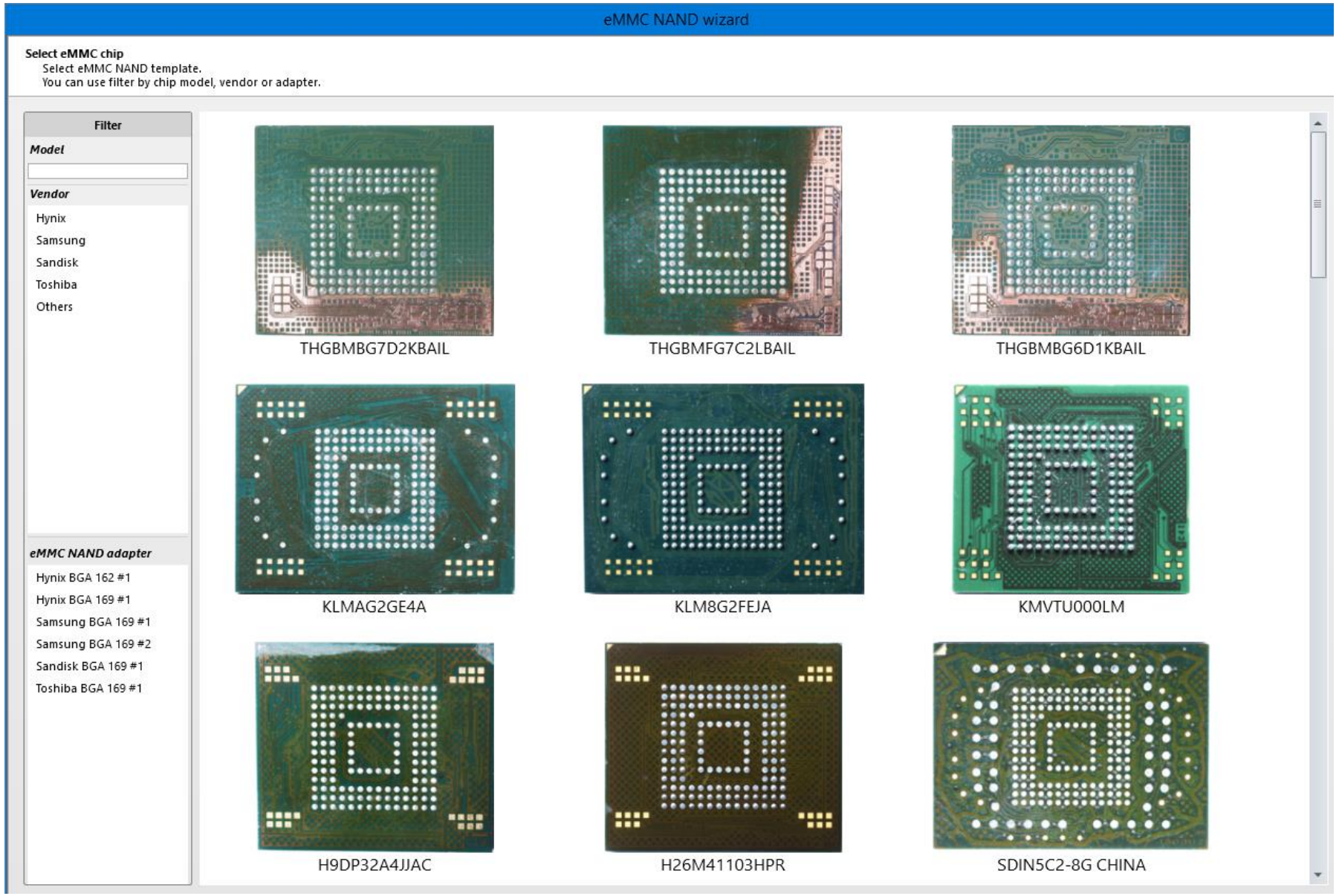
NAND PINOUT



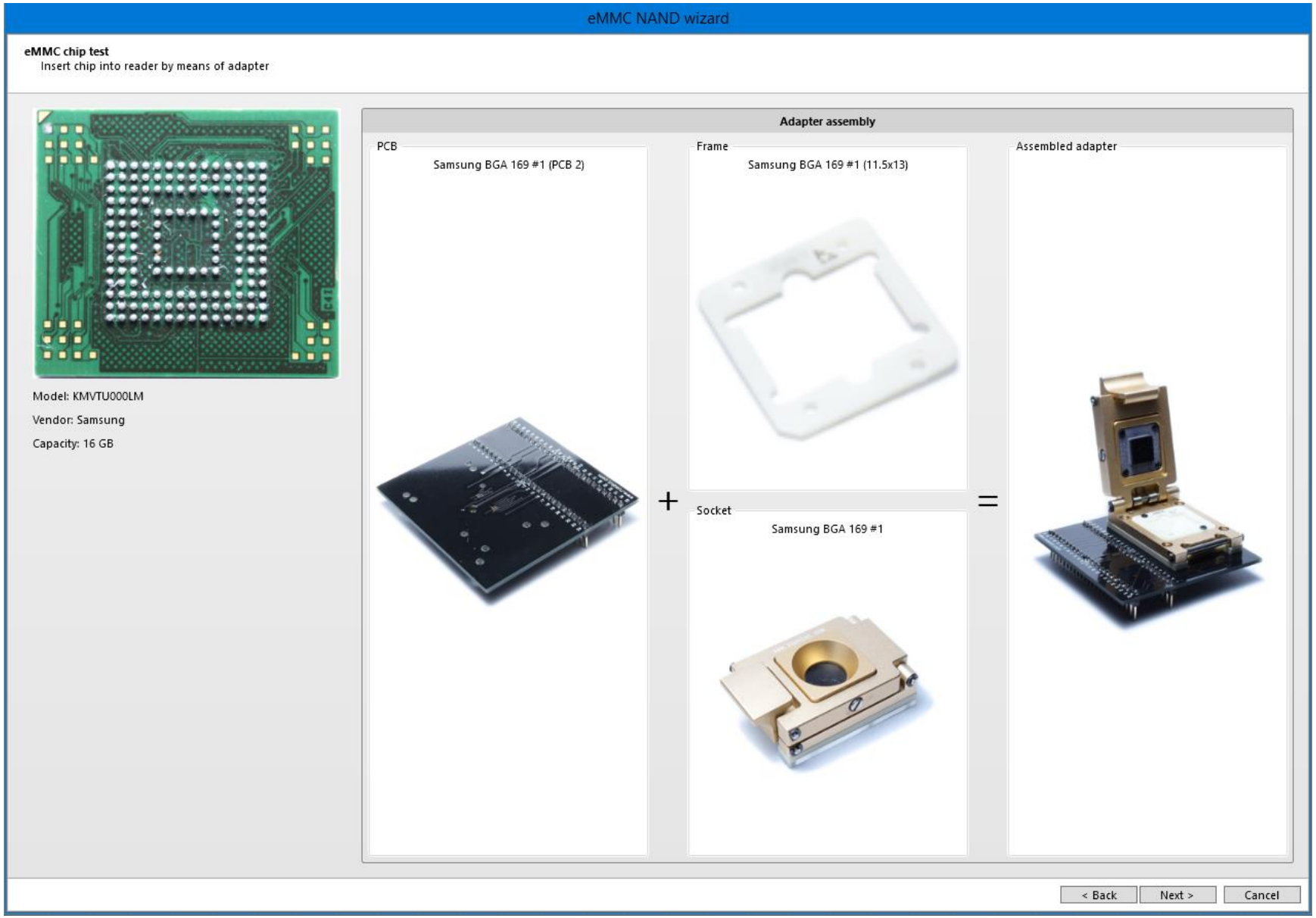
CONNECT CHIP TO ADAPTER

ruSolut

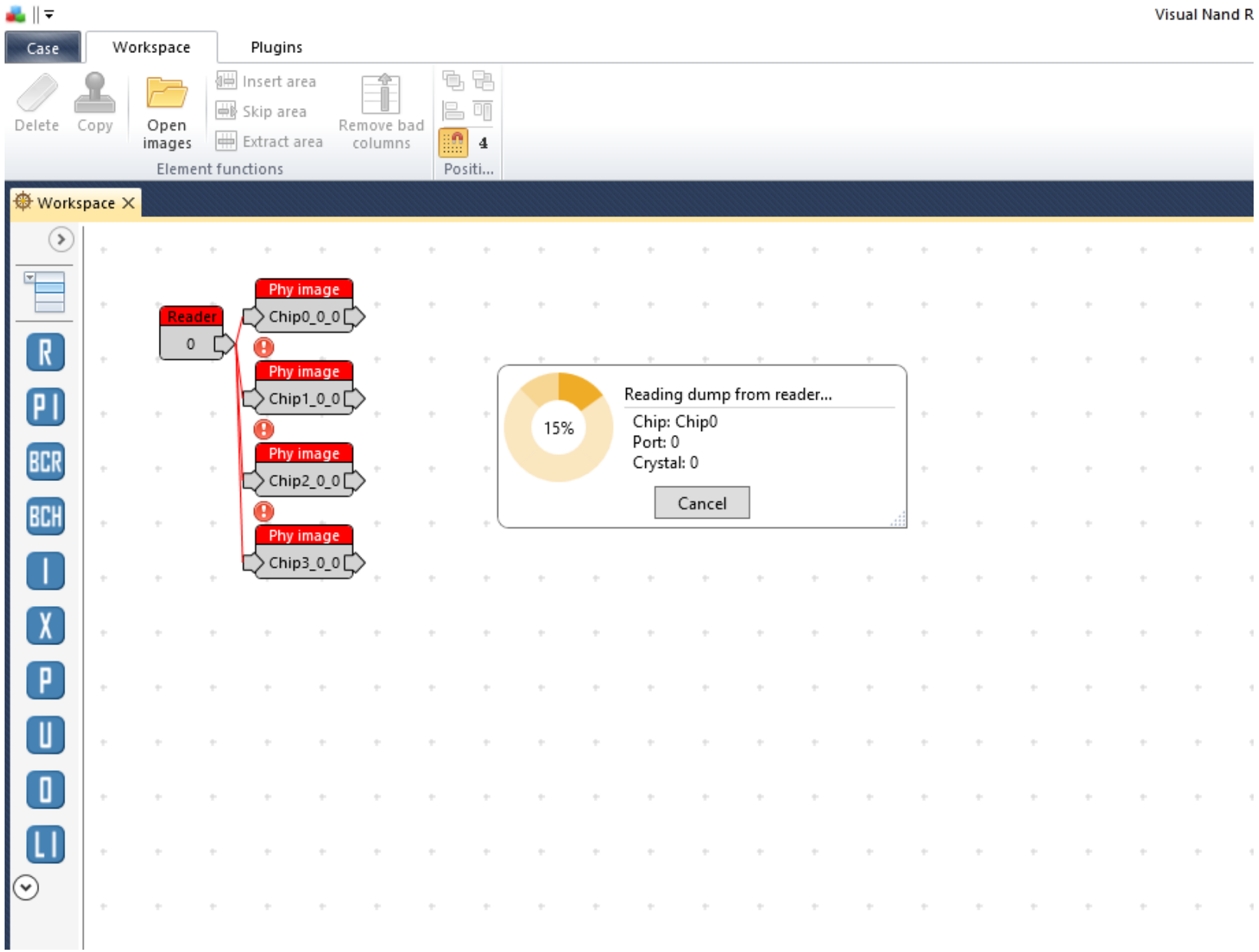
VISUAL NAND RECONSTRUCOR – THE NEW MODE FOR EMMC-NAND ACCESS



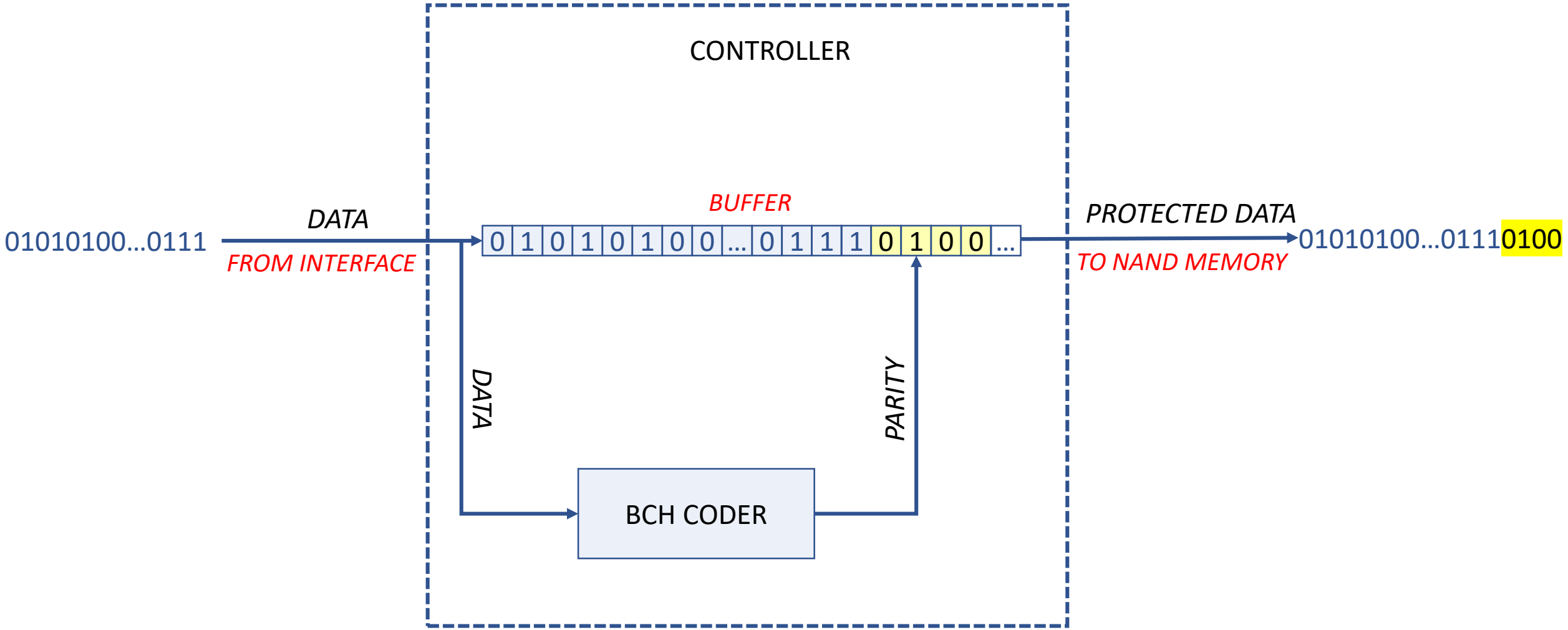
ADAPTER ASSEMBLY



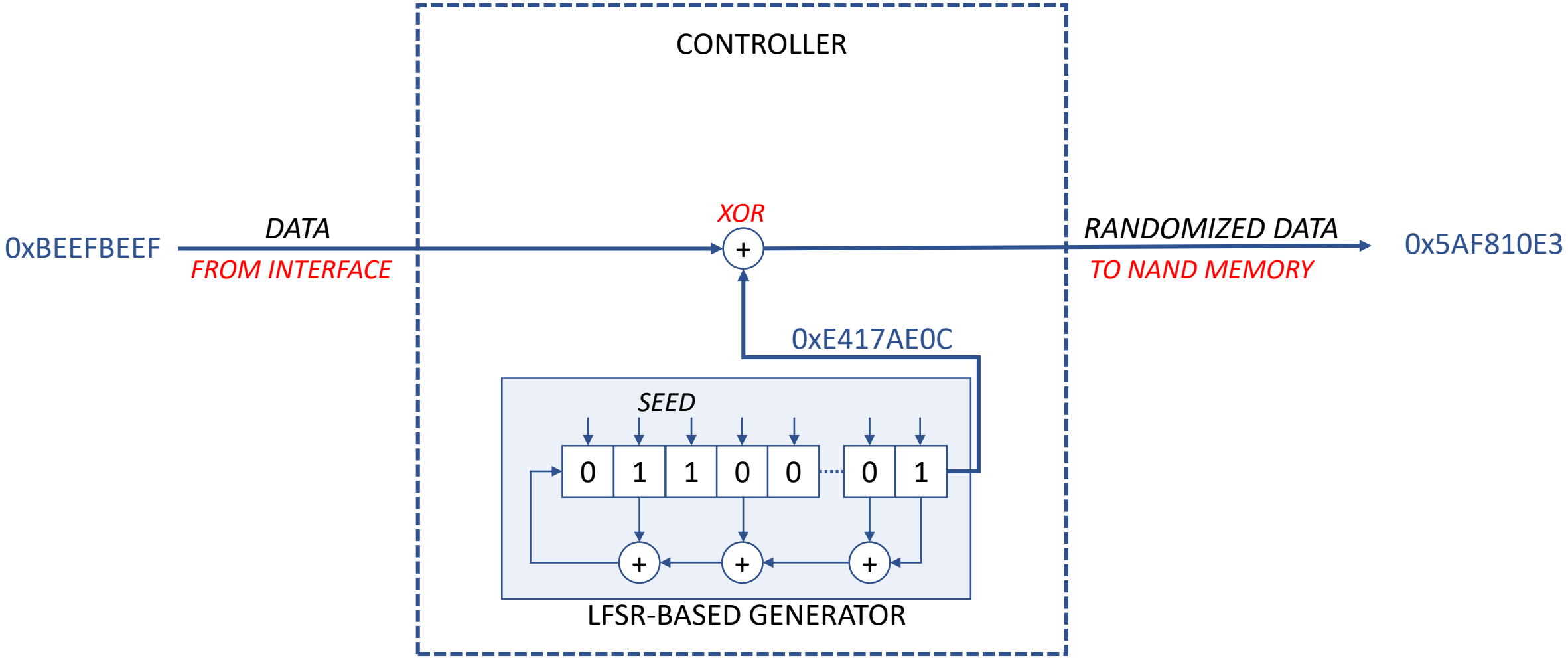
RAW NAND PHYSICAL IMAGE EXTRACTION



ERROR CORRECTION CODES IN FLASH MEMORY



DATA SCRAMBLERS OF FLASH CONTROLLERS



LOGICAL IMAGE RECONSTRUCTION

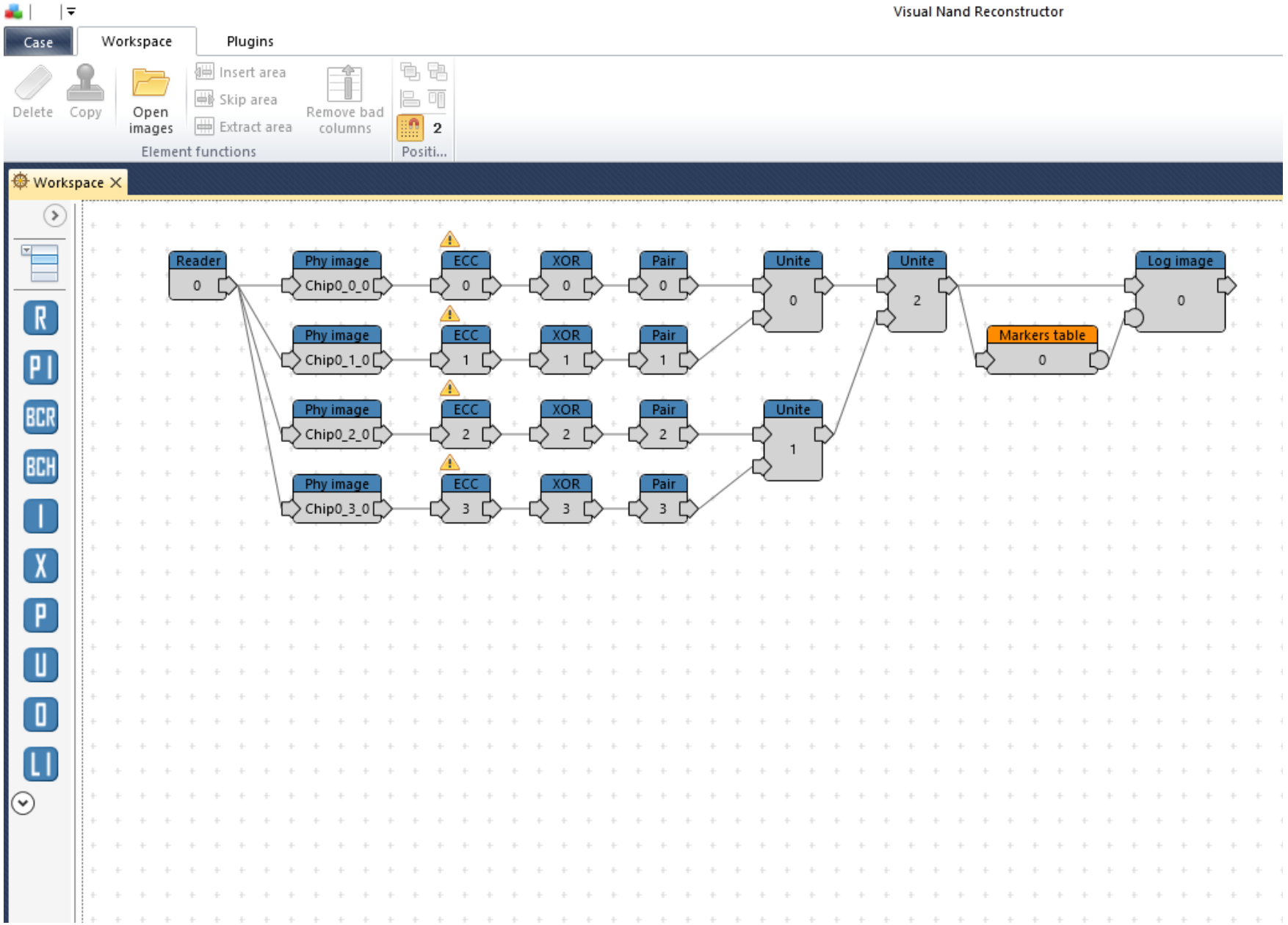
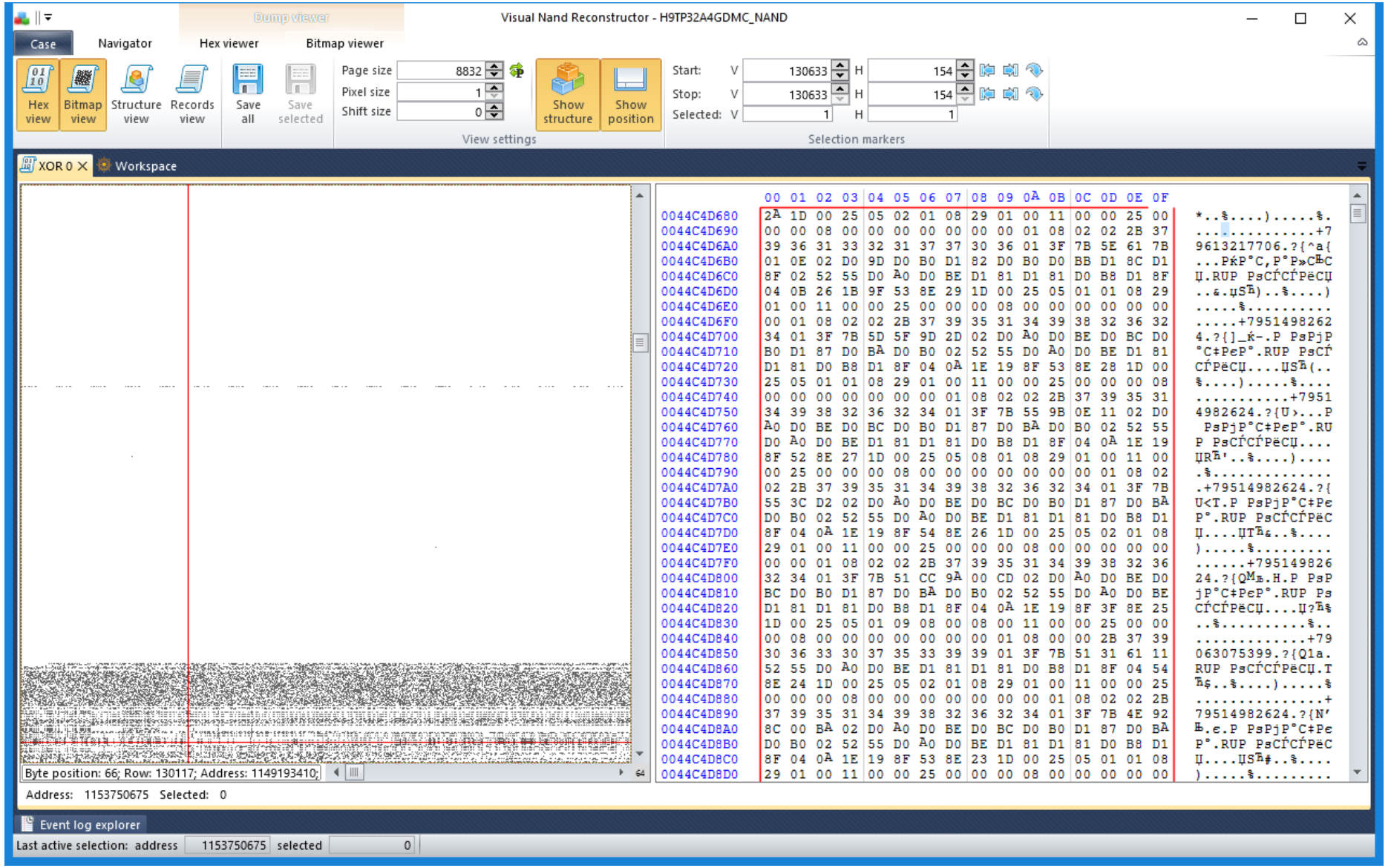


IMAGE AFTER DESCRAMBLING

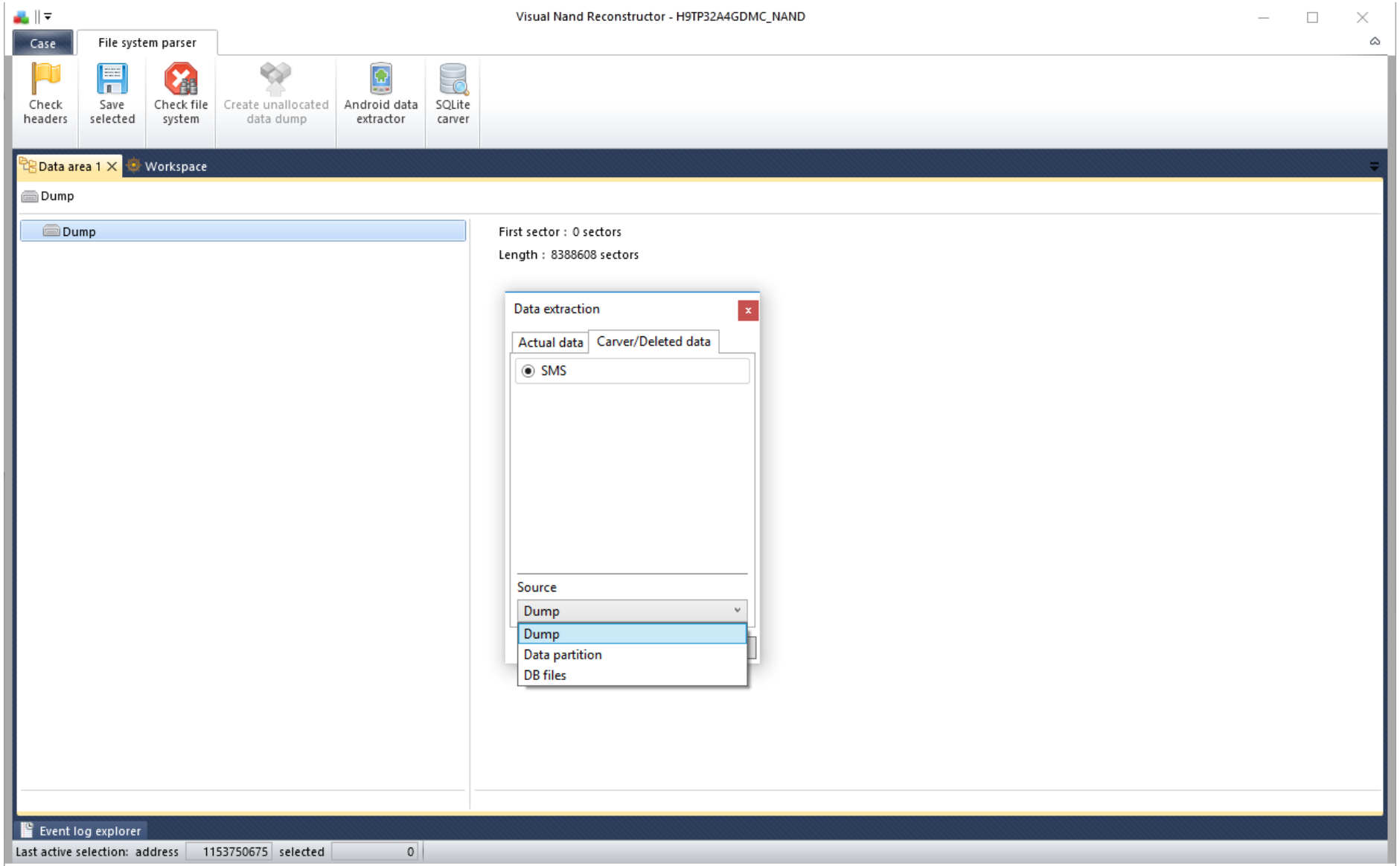
REMEMBER WE ZEROED THIS DEVICE? WE EXPECT TO SEE 0x00 IN EVERY SECTOR/PAGE. BUT WHAT WE ACTUALLY SEE IS A BIT DIFFERENT:

- AFTER 1ST ERASE CYCLE ~5% OF BLOCKS WEREN'T ERASED
- AFTER 2ND ERASE CYCLE ~1% OF BLOCKS WEREN'T ERASED

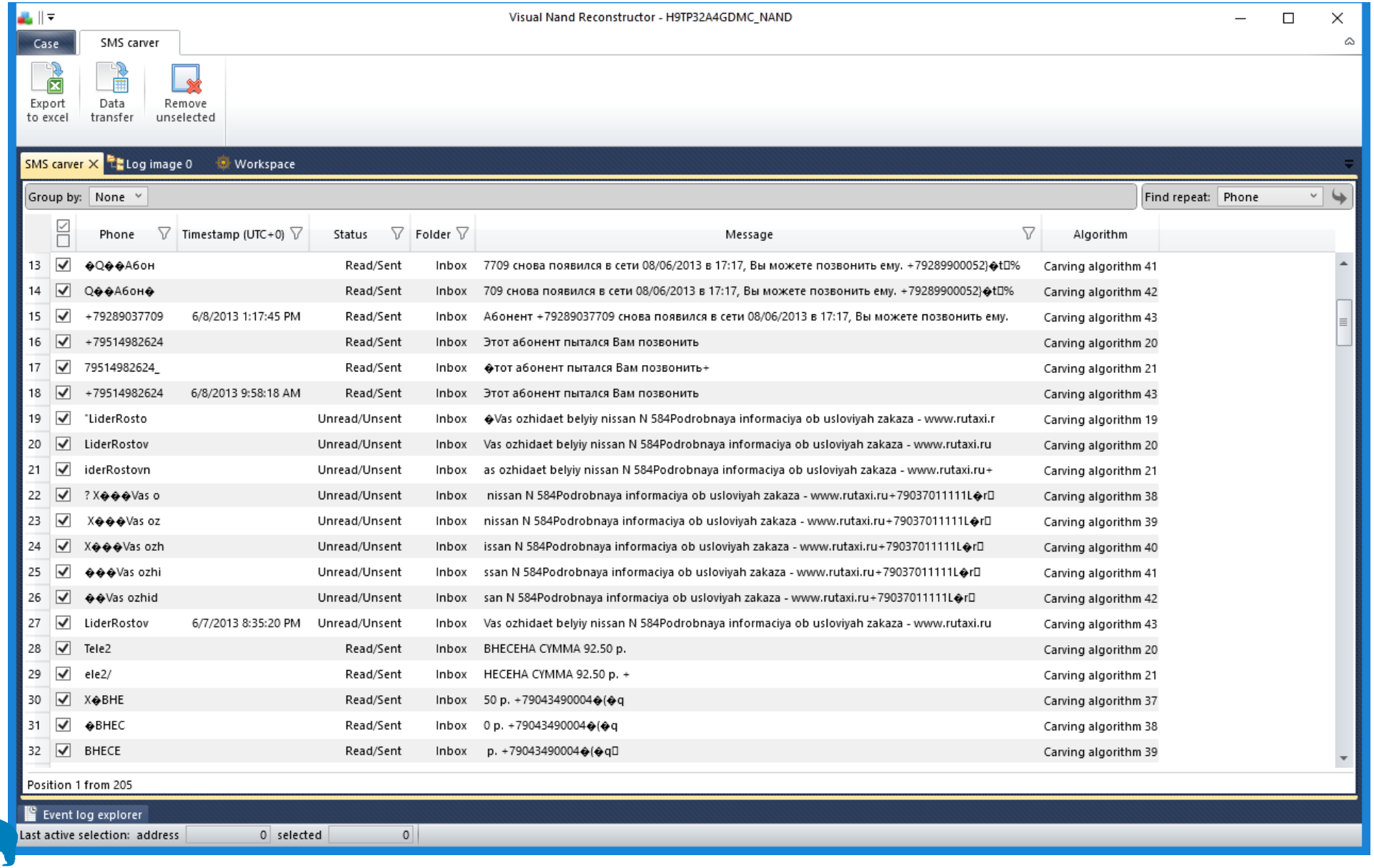


SMS CARVING

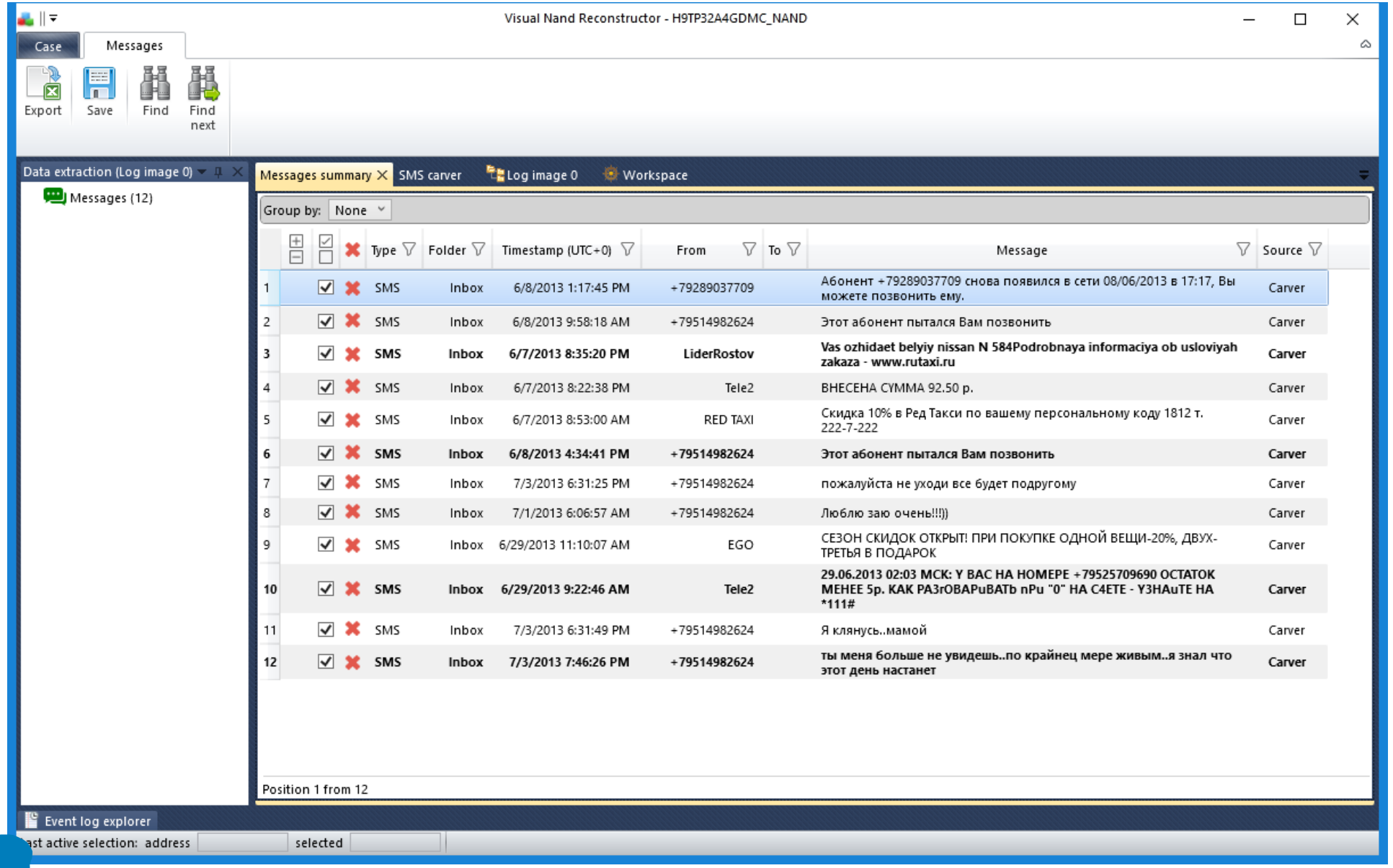
THE MOST INTERESTING PART. ARE THERE REALLY ANY MESSAGES?



RAW CARVING RESULTS



CLEANED UP RESULTS



OUR THEORY IS PROVED. BUT NOBODY WANTS TO ERASE eMMC CHIP IN REAL LIFE.

WE CAN POSSIBLY GET MORE DATA FROM EVERY eMMC VIA NAND PROTOCOL?!

SMS RECOVERY FROM 10 SMARTPHONES (SAME MODEL)

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) during read operation

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%

ruSolut

APPLICATIONS OF TECHNOLOGY

- DATA RECOVERY FROM DAMAGED EMMC CHIPS

- RETRIEVAL OF DELETED TEXT MESSAGES, CHATS , ETC. THROUGH NAND PROTOCOL INCLUDING GARBAGE BLOCKS ON DEEPER LEVEL THAT IS NOT ACCESSIBLE FOR CLASSIC MOBILE FORENSIC TOOLS

- DATA RECOVERY AFTER FACTORY RESET OR OTHER OPERATIONS THAT ERASE DATA

Related links:
https://rusolut.com/wp-content/uploads/2018/06/Sheremetov-The-Ultimate-Chip-off-Mobile-Forensics.-Data-Resurrection-from-Dead-eMMC-Chips-June-3-Oleander-B.pdf
https://www.flashmemorysummit.com/English/Collaterals/Proceedings/2017/20170808_S102A_Sheremetov.pdf
https://belkasoft.com/ssd-2016-part2

THANK YOU

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

ruSolut