eMMC-NAND RECONSTRUCTOR

Alexander (Sasha) Sheremetov - Rusolut

ruSolut

APPLICATIONS OF EMMC CHIPS IS WIDE

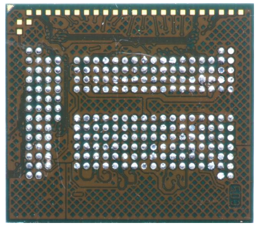
- SMARTPHONES
- TABLETS
- DRONES
- CARS
- SATNAV SYSTEMS
- WEARABLES/SMARTWATCH
- LAPTOPS
- VOICE RECORDERS
- MULTIMEDIA PLAYERS
- TV BOXES
- SMART TV
- INTERNET OF THINGS

…AND MUCH MORE…

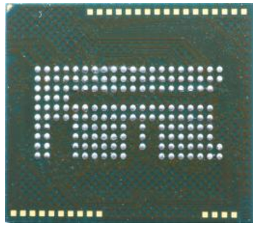
ruSolut

COMMON EMMC/EMCP CHIPS USED IN PHONES AND OTHER DEVICES

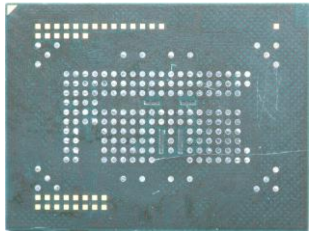
BGA221



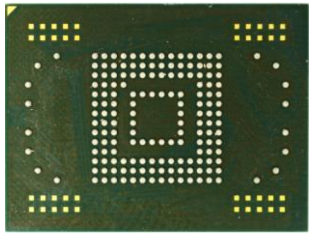
BGA162



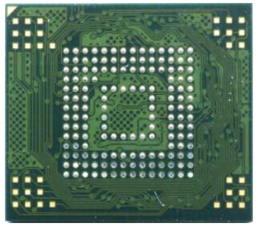
BGA186



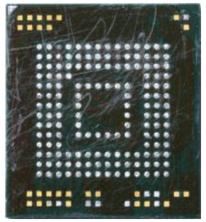
BGA169 12x16



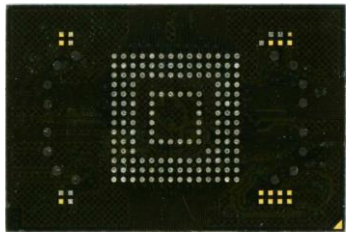
BGA153/169 11,5x13



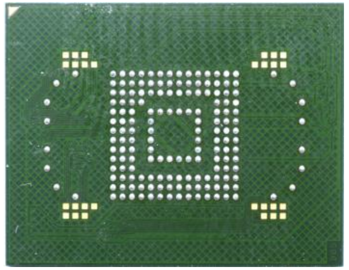
BGA153/169 10x11



BGA169 12x18

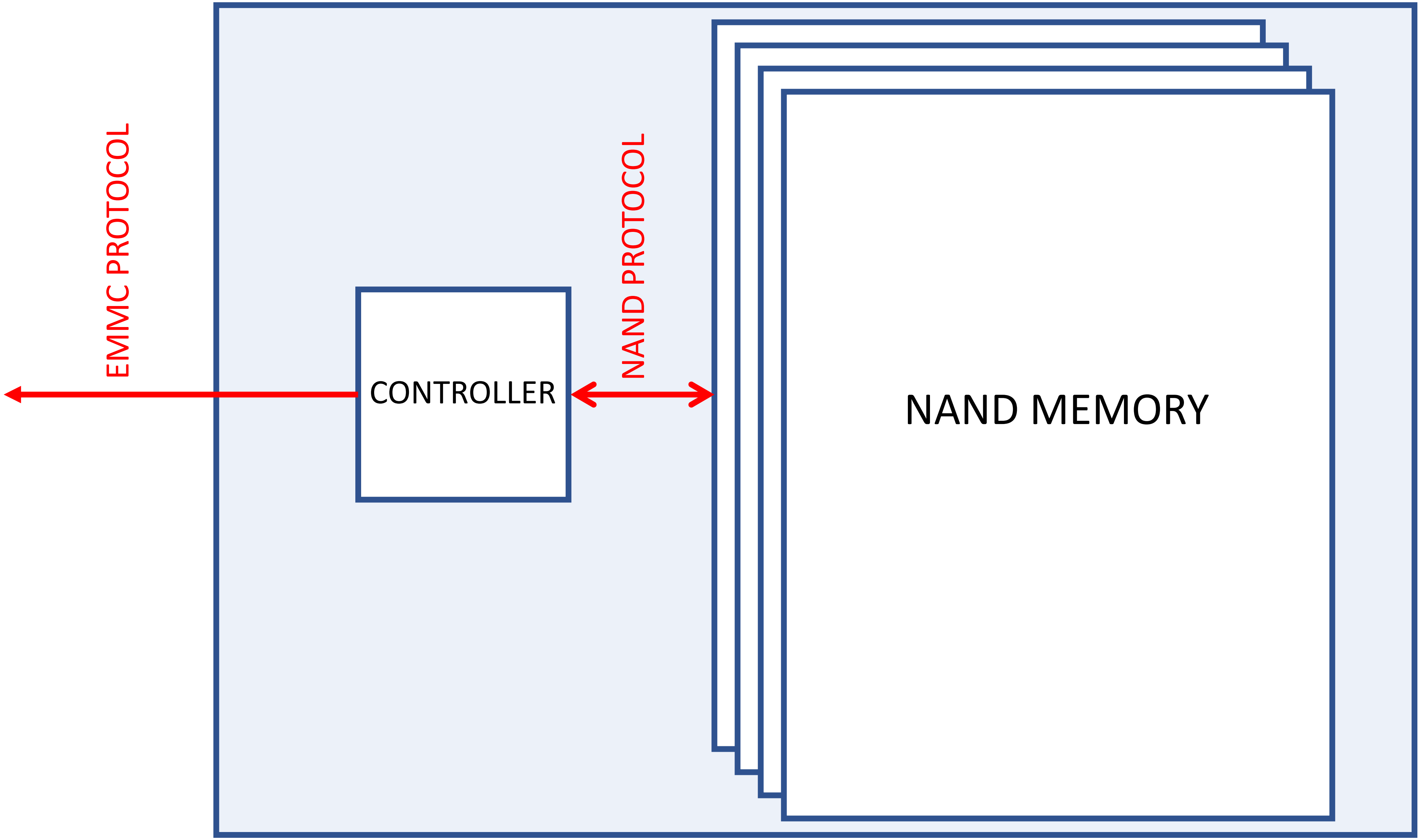


BGA169 14x18



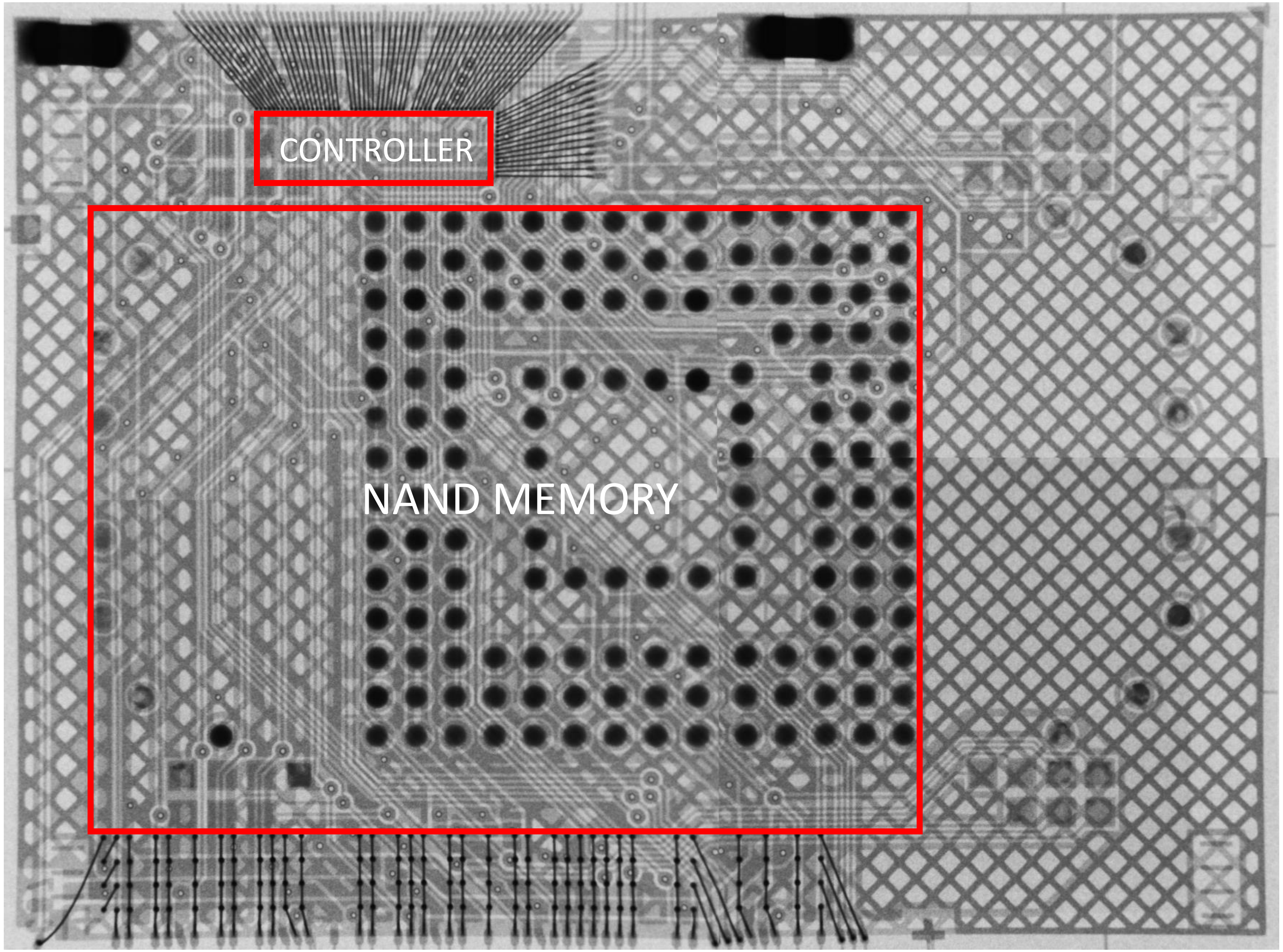
ruSolut

INSIDE EMMC

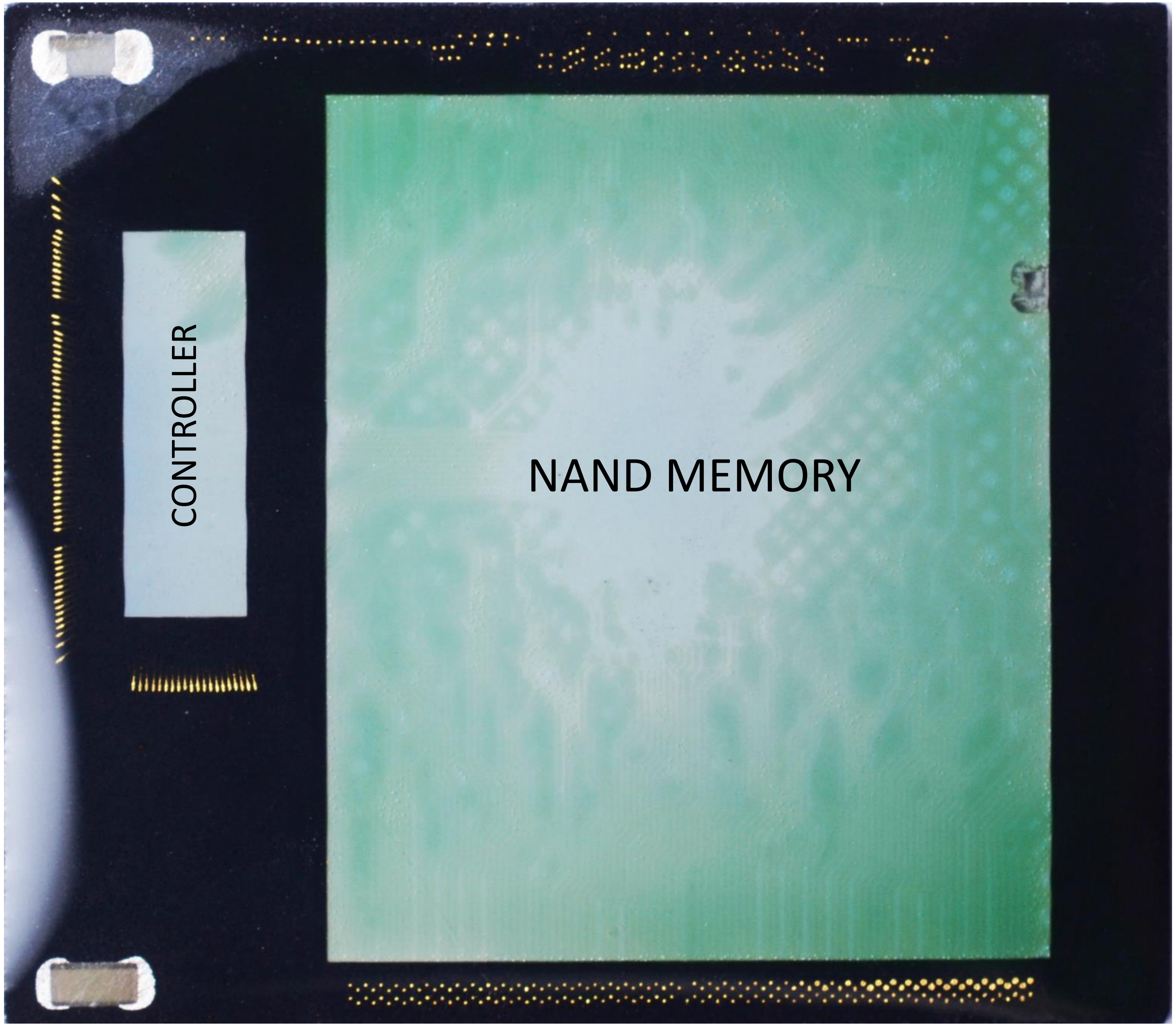


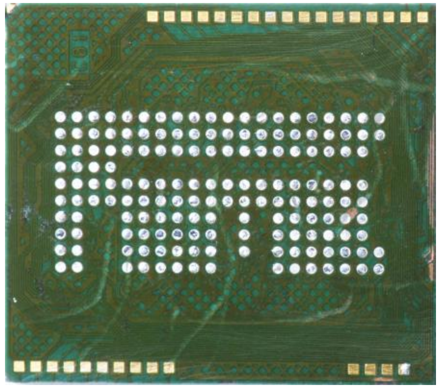
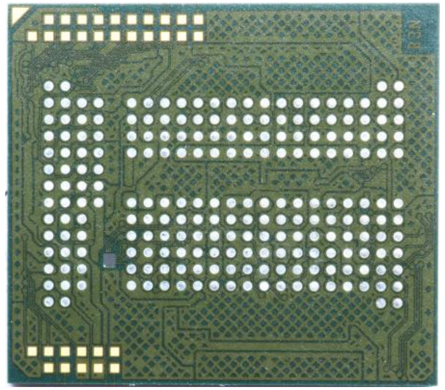
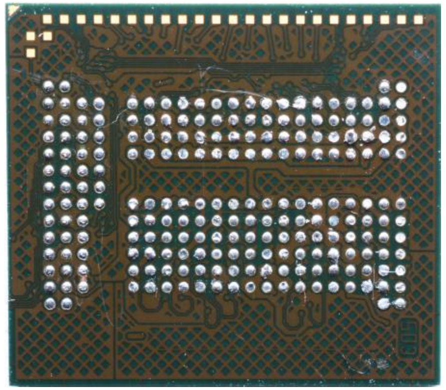
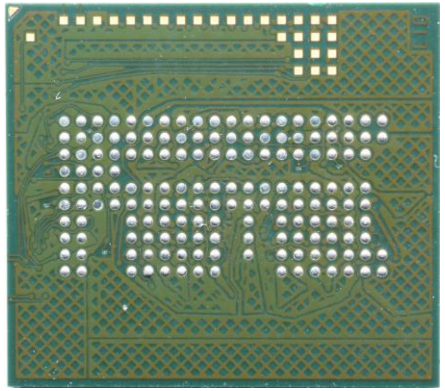
ruSolut

EMMC THROUGH XRAY

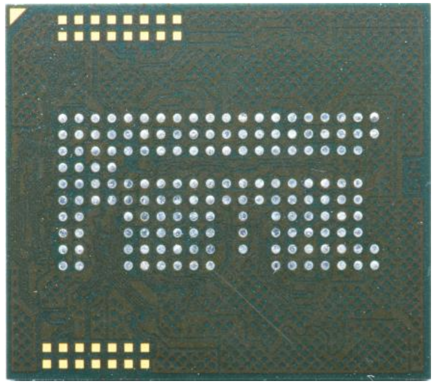
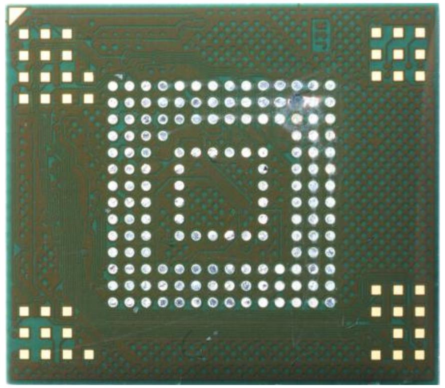
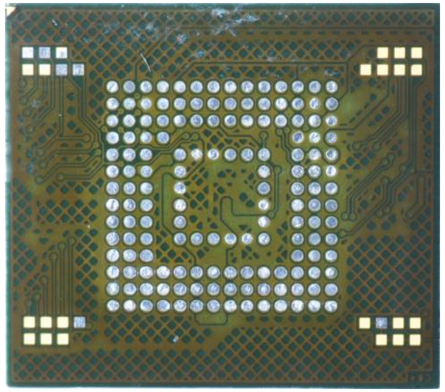
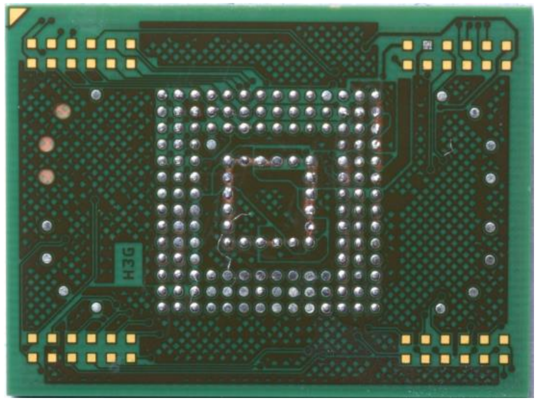


EMMC - CHIP LAYER



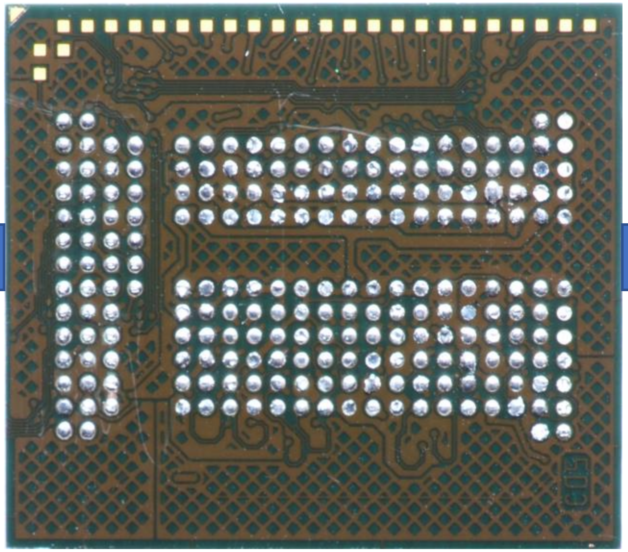
TECHNOLOGICAL PADS - NAND INTERFACE

WHY CARE ABOUT GETTING PHYSICAL IMAGE THROUGH NAND?

- QUICK EXTRACTION
- WORKING CHIPS
- LOGICAL IMAGE (95-97% OF DATA)

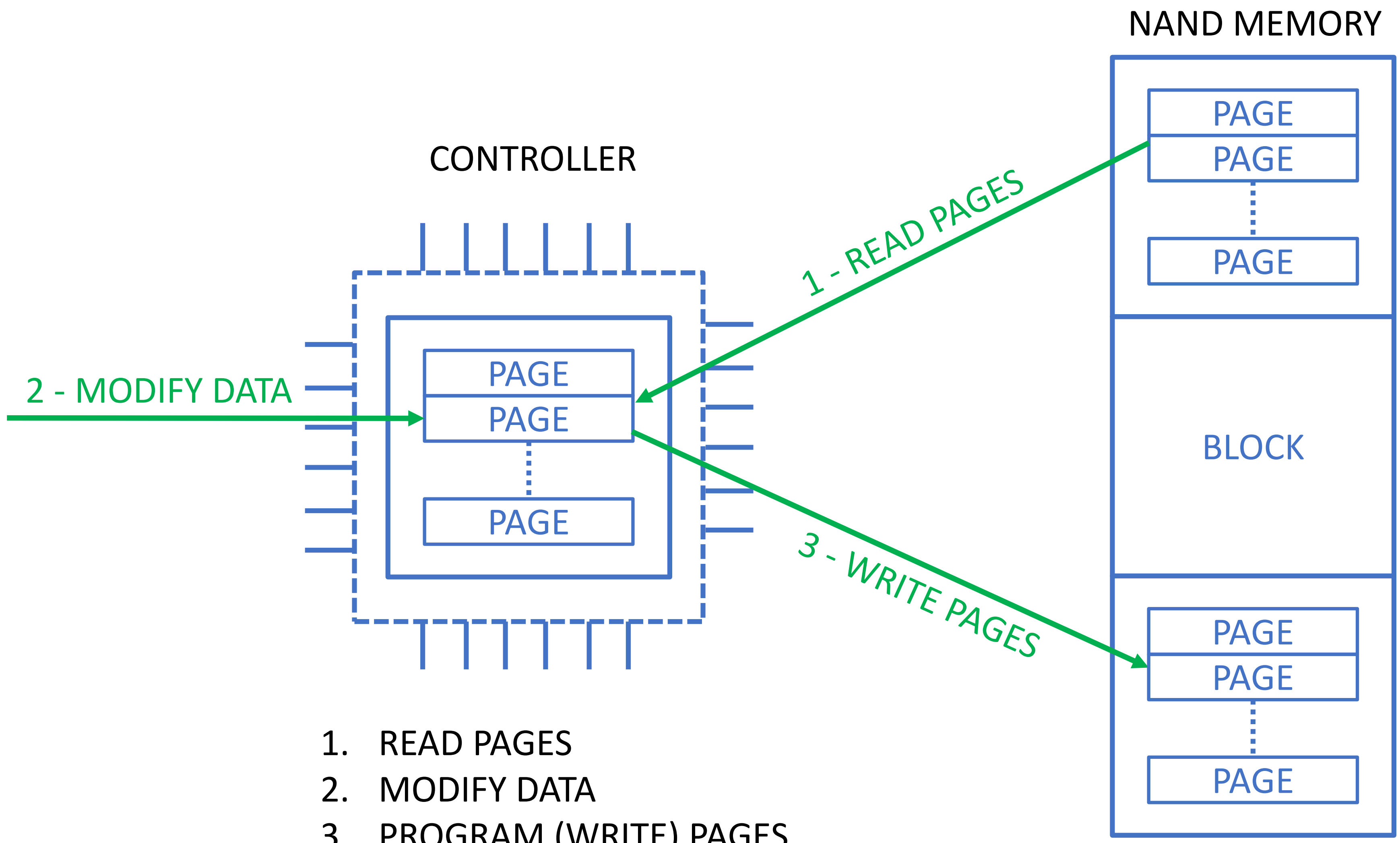
eMMC



NAND

- DEEP EXTRACTION OF DELETED DATA
- DATA EXTRACTION EVEN AFTER RESET
- DEAD CHIPS
- TRUE PHYSICAL IMAGE (100% OF DATA)

DATA RECOVERY FROM GARBAGE BLOCKS OF NAND



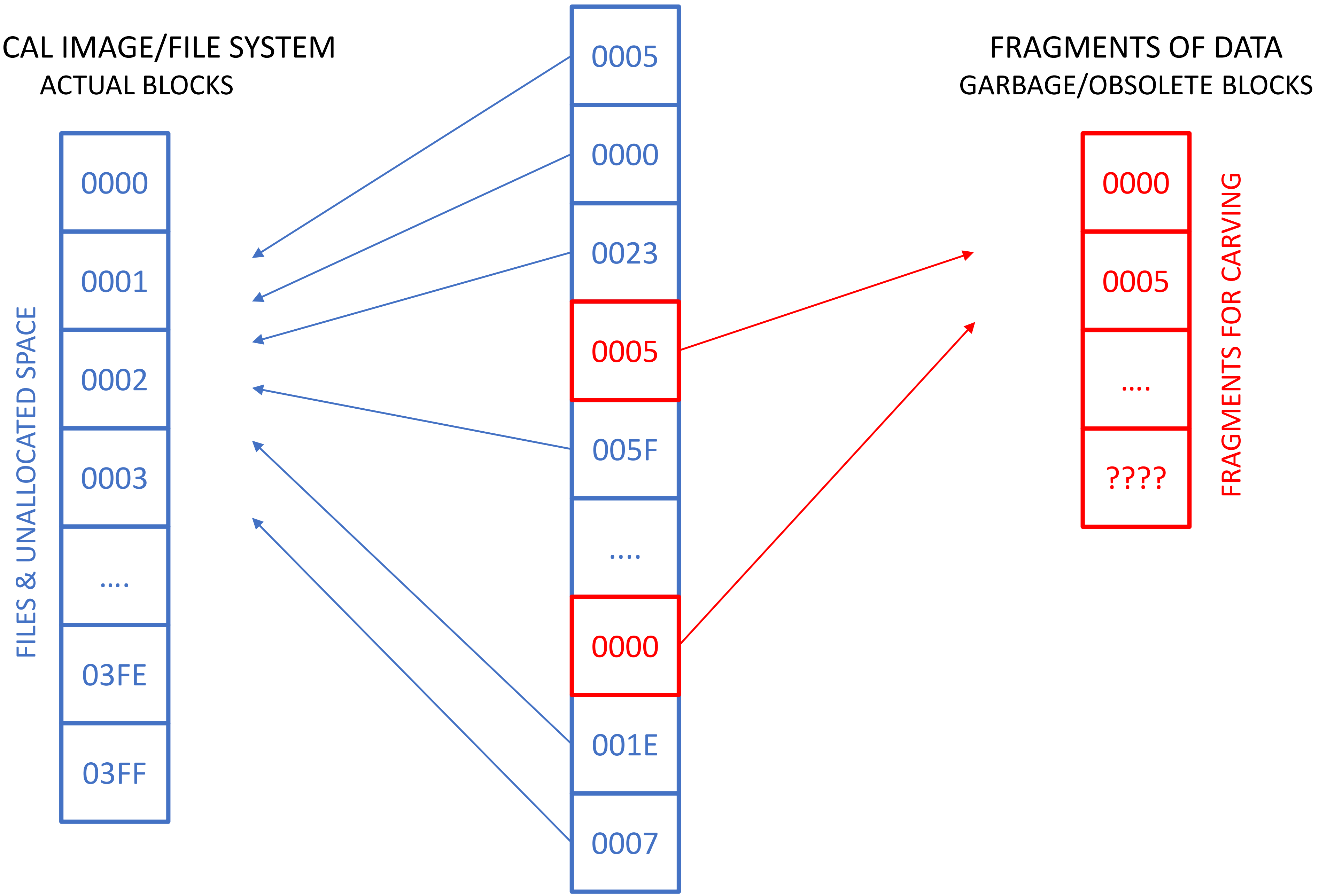
OLD UNERASED BLOCK STAYS UNTOUCHED FOR SOME TIME UNTIL GARBAGE COLLECTION ALGORITHM ERASE IT. USUALLY IT'S NOT FAST PROCESS

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

PHYSICAL IMAGE

LOGICAL IMAGE/FILE SYSTEM
ACTUAL BLOCKS

FRAGMENTS OF DATA
GARBAGE/OBSOLETE BLOCKS



FILES & UNALLOCATED SPACE

0000
0001
0002
0003
….
03FE
03FF

0005
0000
0023
0005
005F
….
0000
001E
0007

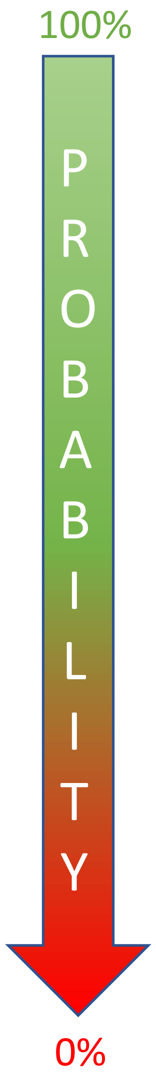
0000
0005
….
????

FRAGMENTS FOR CARVING

HOW MANY GARBAGE BLOCKS CAN WE FIND IN AVERAGE DUMP?

FROM SEVERAL BLOCKS TO SEVERAL DOZENS

WHAT CAN/CANNOT BE CARVED FROM THE FRAGMENTS, REALISTICALLY



100%

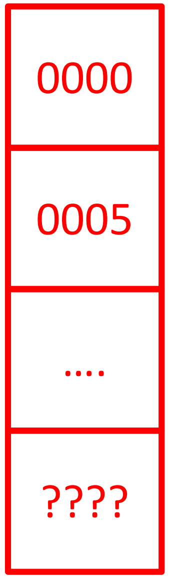
PROBABILITY

0%

- SMS
- CHATS
- GPS DATA
- EMAILS
- CONTACTS
- LOGS
- TEXT DATA
- THUMBNAILS
- PICTURES
- ZIP
- AUDIO
- VIDEO

SIZE OF SEQUENTIAL CHUNKS OF DATA
VARIES FROM ONE PAGE TO ONE BLOCK
WHICH TRANSLATES TO:
8KB … 4MB

GARBAGE/OBSOLETE BLOCKS



0000

0005

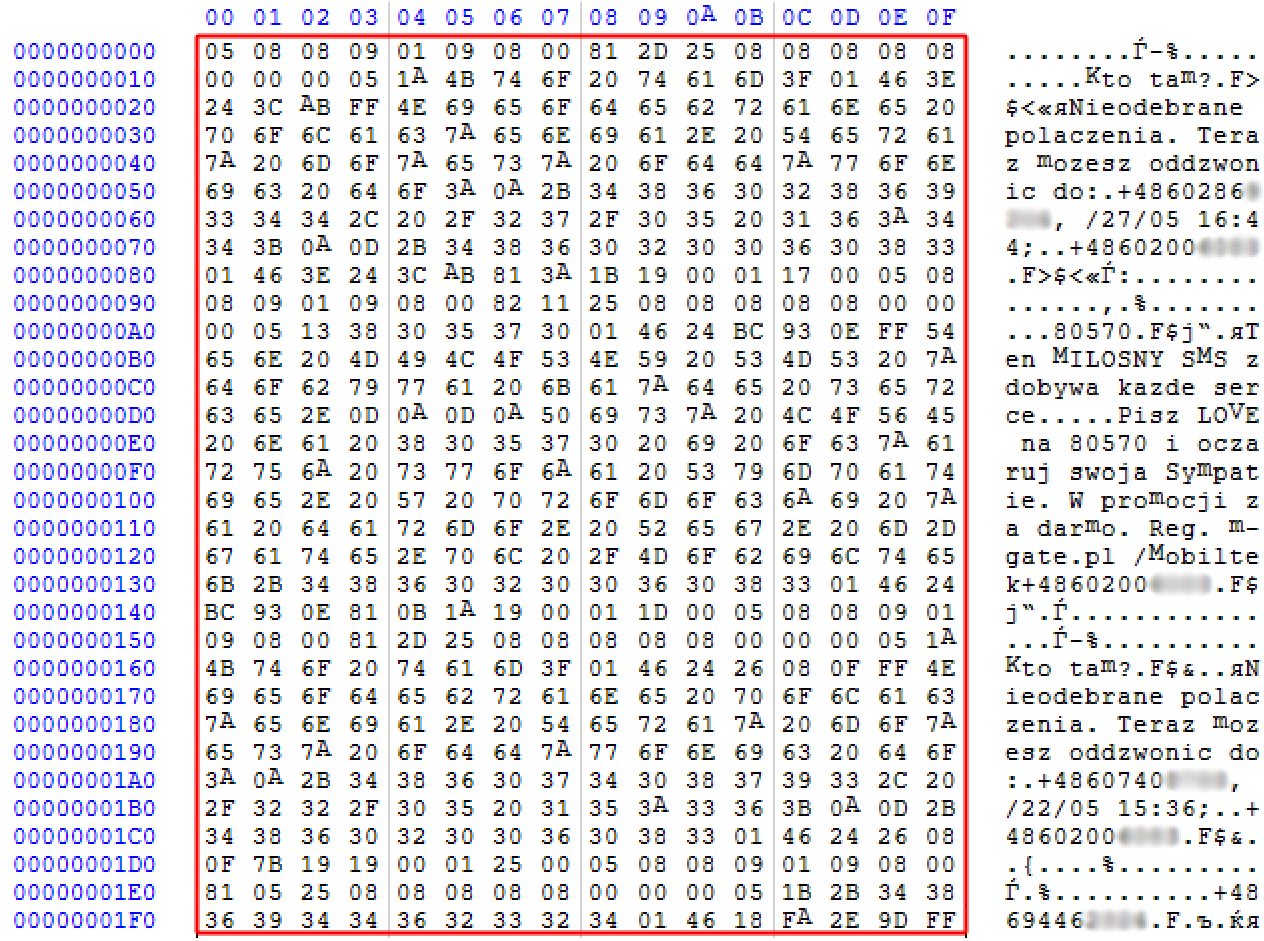
….

????

ruSolut

8KB FRAGMENT OF DATA…IS IT A LOT? HOW MUCH EXACTLY?

512 BYTES OF DATA FROM OBSOLETE PAGE



```
            00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
0000000000  05 08 08 09 01 09 08 00 81 2D 25 08 08 08 08 08   ........Ѓ-%.....
0000000010  00 00 00 05 1A 4B 74 6F 20 74 61 6D 3F 01 46 3E   .....Kto tam?.F>
0000000020  24 3C AB FF 4E 69 65 6F 64 65 62 72 61 6E 65 20   $<«яNieodebrane 
0000000030  70 6F 6C 61 63 7A 65 6E 69 61 2E 20 54 65 72 61   polaczenia. Tera
0000000040  7A 20 6D 6F 7A 65 73 7A 20 6F 64 64 7A 77 6F 6E   z mozesz oddzwon
0000000050  69 63 20 64 6F 3A 0A 2B 34 38 36 30 32 38 36 39   ic do:.+4860286[redacted]
0000000060  33 34 34 2C 20 2F 32 37 2F 30 35 20 31 36 3A 34   [redacted], /27/05 16:4
0000000070  34 3B 0A 0D 2B 34 38 36 30 32 30 30 36 30 38 33   4;..+4860200[redacted]
0000000080  01 46 3E 24 3C AB 81 3A 1B 19 00 01 17 00 05 08   .F>$<«Ѓ:........
0000000090  08 09 01 09 08 00 82 11 25 08 08 08 08 08 00 00   ......,.%.......
00000000A0  00 05 13 38 30 35 37 30 01 46 24 BC 93 0E FF 54   ...80570.F$j".яT
00000000B0  65 6E 20 4D 49 4C 4F 53 4E 59 20 53 4D 53 20 7A   en MILOSNY SMS z
00000000C0  64 6F 62 79 77 61 20 6B 61 7A 64 65 20 73 65 72   dobywa kazde ser
00000000D0  63 65 2E 0D 0A 0D 0A 50 69 73 7A 20 4C 4F 56 45   ce.....Pisz LOVE
00000000E0  20 6E 61 20 38 30 35 37 30 20 69 20 6F 63 7A 61    na 80570 i ocza
00000000F0  72 75 6A 20 73 77 6F 6A 61 20 53 79 6D 70 61 74   ruj swoja Sympat
0000000100  69 65 2E 20 57 20 70 72 6F 6D 6F 63 6A 69 20 7A   ie. W promocji z
0000000110  61 20 64 61 72 6D 6F 2E 20 52 65 67 2E 20 6D 2D   a darmo. Reg. m-
0000000120  67 61 74 65 2E 70 6C 20 2F 4D 6F 62 69 6C 74 65   gate.pl /Mobilte
0000000130  6B 2B 34 38 36 30 32 30 30 36 30 38 33 01 46 24   k+4860200[redacted].F$
0000000140  BC 93 0E 81 0B 1A 19 00 01 1D 00 05 08 08 09 01   j".Ѓ............
0000000150  09 08 00 81 2D 25 08 08 08 08 08 00 00 00 05 1A   ...Ѓ-%..........
0000000160  4B 74 6F 20 74 61 6D 3F 01 46 24 26 08 0F FF 4E   Kto tam?.F$&..яN
0000000170  69 65 6F 64 65 62 72 61 6E 65 20 70 6F 6C 61 63   ieodebrane polac
0000000180  7A 65 6E 69 61 2E 20 54 65 72 61 7A 20 6D 6F 7A   zenia. Teraz moz
0000000190  65 73 7A 20 6F 64 64 7A 77 6F 6E 69 63 20 64 6F   esz oddzwonic do
00000001A0  3A 0A 2B 34 38 36 30 37 34 30 38 37 39 33 2C 20   :.+4860740[redacted], 
00000001B0  2F 32 32 2F 30 35 20 31 35 3A 33 36 3B 0A 0D 2B   /22/05 15:36;..+
00000001C0  34 38 36 30 32 30 30 36 30 38 33 01 46 24 26 08   4860200[redacted].F$&.
00000001D0  0F 7B 19 19 00 01 25 00 05 08 08 09 01 09 08 00   .{....%.........
00000001E0  81 05 25 08 08 08 08 08 00 00 00 05 1B 2B 34 38   Ѓ.%.........+48
00000001F0  36 39 34 34 36 32 33 32 34 01 46 18 FA 2E 9D FF   69446[redacted].F.ъ.ќя
```

WITHIN 512 BYTES OF DATA WE CAN SEE 3 SMS.

PAGE IS AT LEAST 16 TIMES LARGER.

SIMPLE CALCULATION SHOWS THAT ONE PAGE MAY CONTAIN ROUGHLY 45-50 SMS (OR CHAT MESSAGES).

NOW ASSUME THAT ONE BLOCK IS AT LEAST 128 PAGES.

128 x 45 = 5760.

SO ONE BLOCK MAY CONTAIN ~ 5000 MESSAGES.

ON PRACTISE YOU'LL GET LOTS OF DUPLICATED RECORDS DUE TO THE NATURE OF SQLITE.

SO LET'S JUST SHIRINK IT DOWN TENFOLD TO 500. IT IS STILL A HUGE AMOUNT OF DATA!!!

IS THERE ANY LIFE AFTER FACTORY RESET?

YOU NEVER KNOW UNTIL YOU CHECK IT BUT
AT LEAST GARBAGE BLOCKS ARE RARELY ERASED

DAMAGED EMMC CHIPS

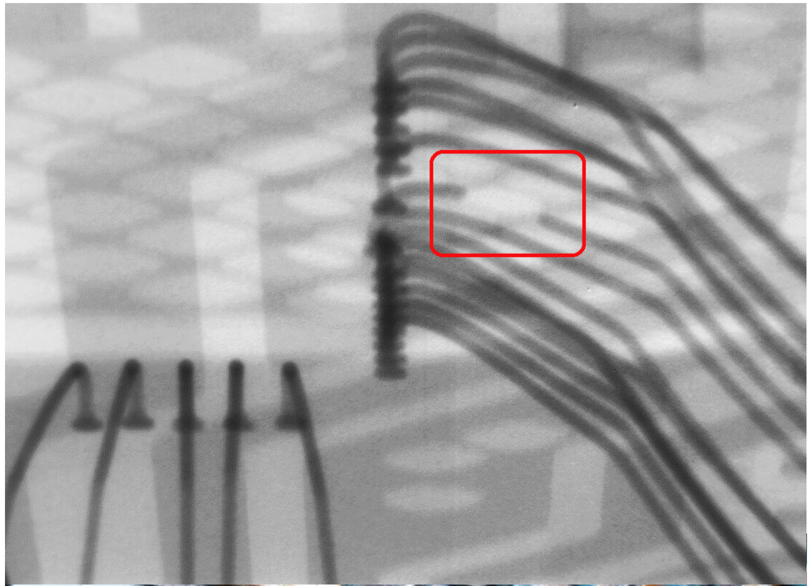
CAUSES

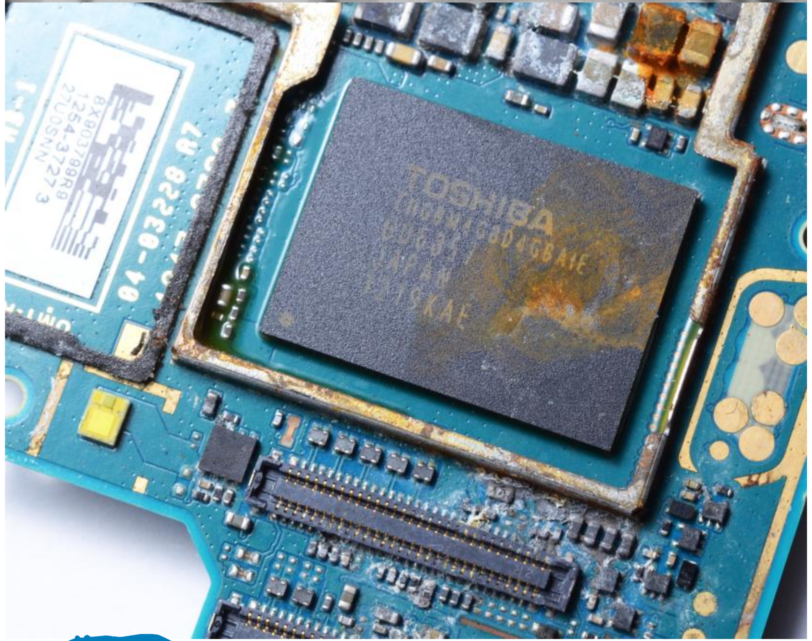
- WATER DAMAGE
- THERMAL DAMAGE
- PHYSICAL DAMAGE
- DAMAGE OF TRACKS/PADS ON CHIP’S PCB
- DAMAGE OF WIRE BONDING INSIDE CHIP
- HUMAN FACTOR DURING DATA RECOVERY

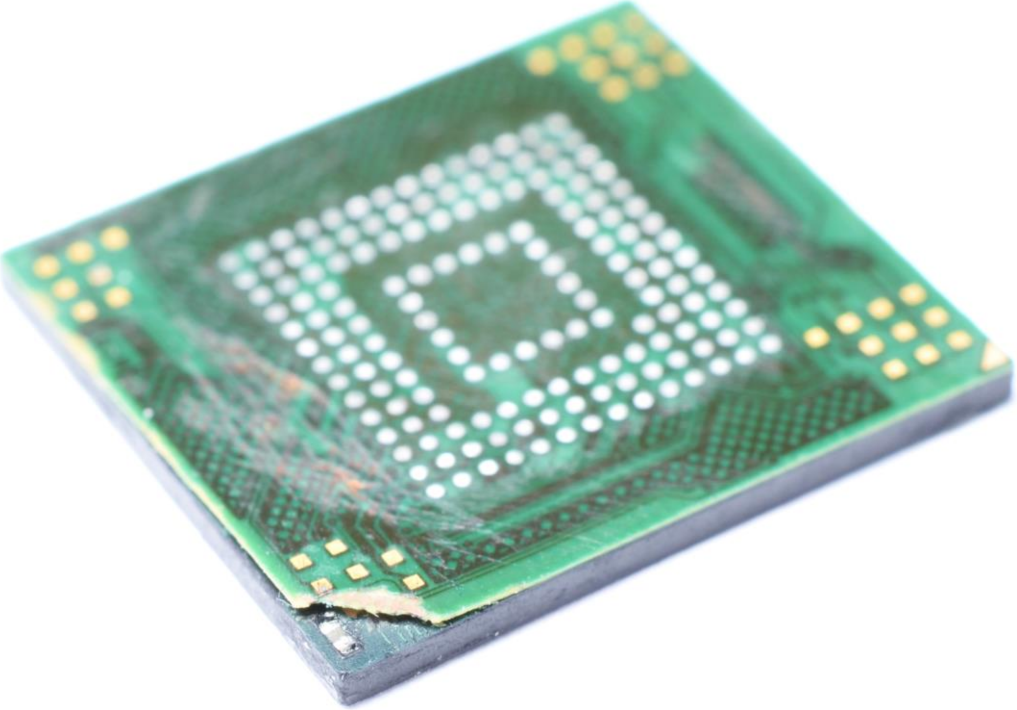
SYMPTOMS

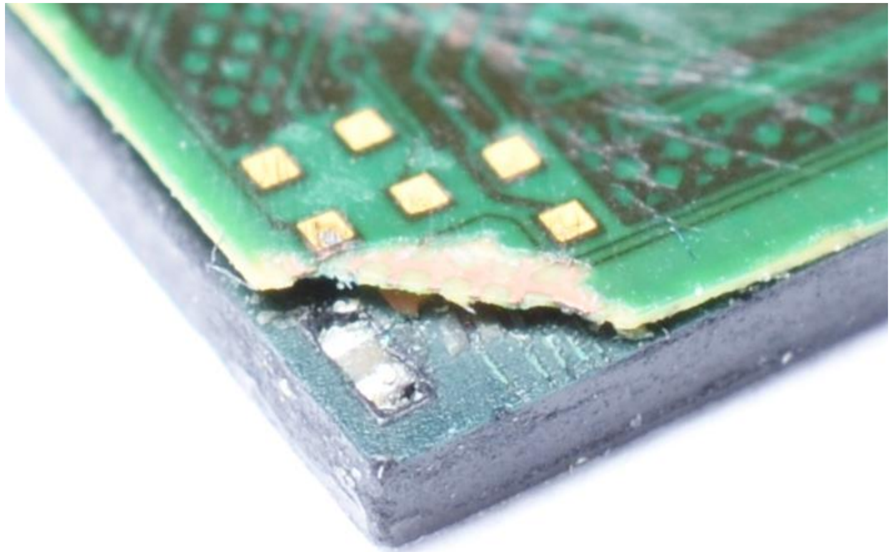
- NOT RECOGNIZED WHEN CONNECTED TO EMMC ADAPTER
- RECOGNIZED BUT SHOWS WEIRD CAPACITY
- RECOGNIZED AND FIRST 32-64MB ACCESSIBLE
- RECOGNIZED BUT READS GARBAGE

DAMAGED EMMC CHIPS









SCENARIOS OF FAILURE

NO SHORT CIRCUIT ~80-90%

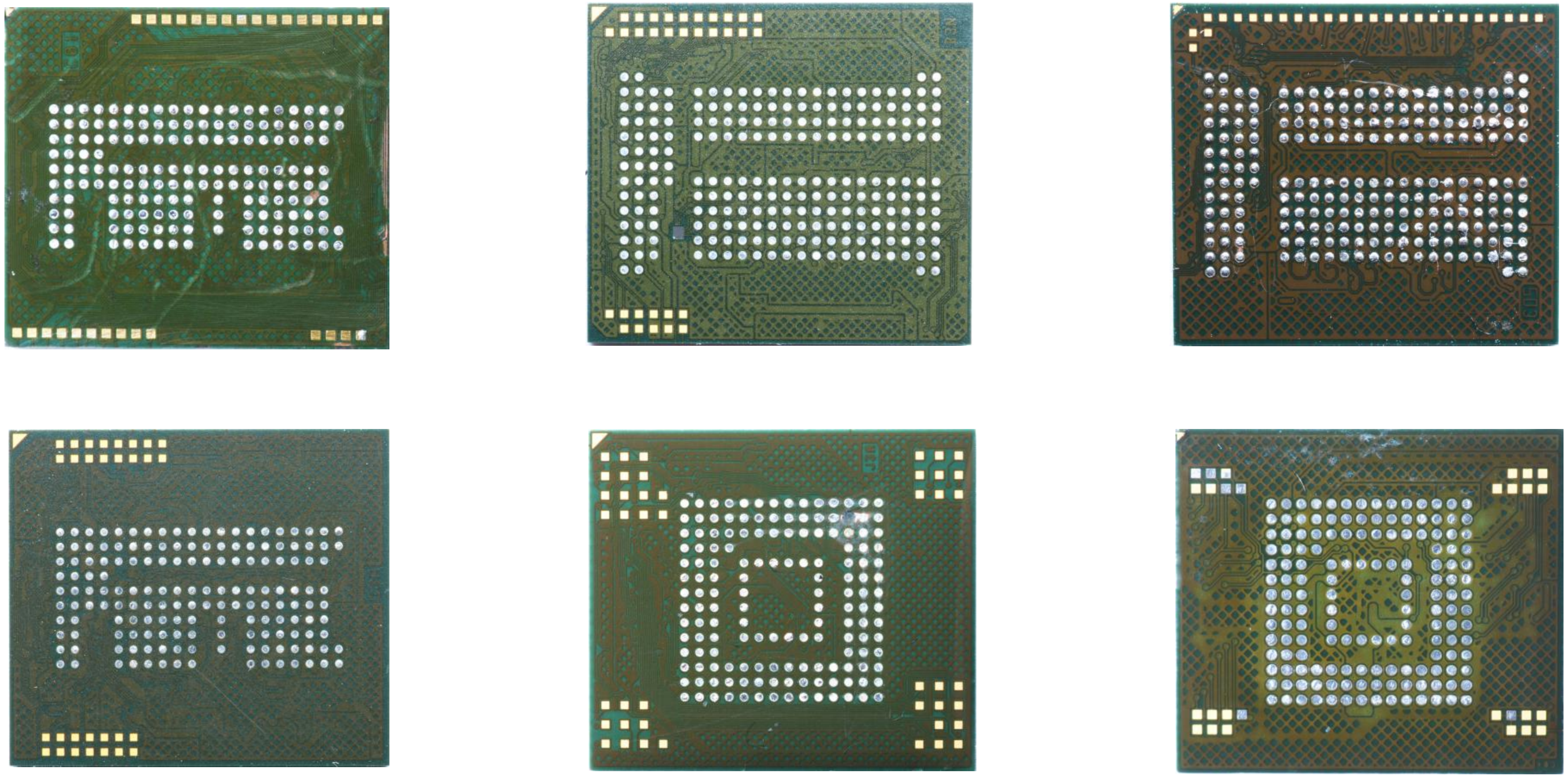
- FW CORRUPTION
- CONTROLLER DAMAGE DUE TO OVERHEAT
- WIRE BONDING DAMAGE
- UNKNOWN COTROLLER DAMAGES

SHORT CIRCUIT ~10-20%

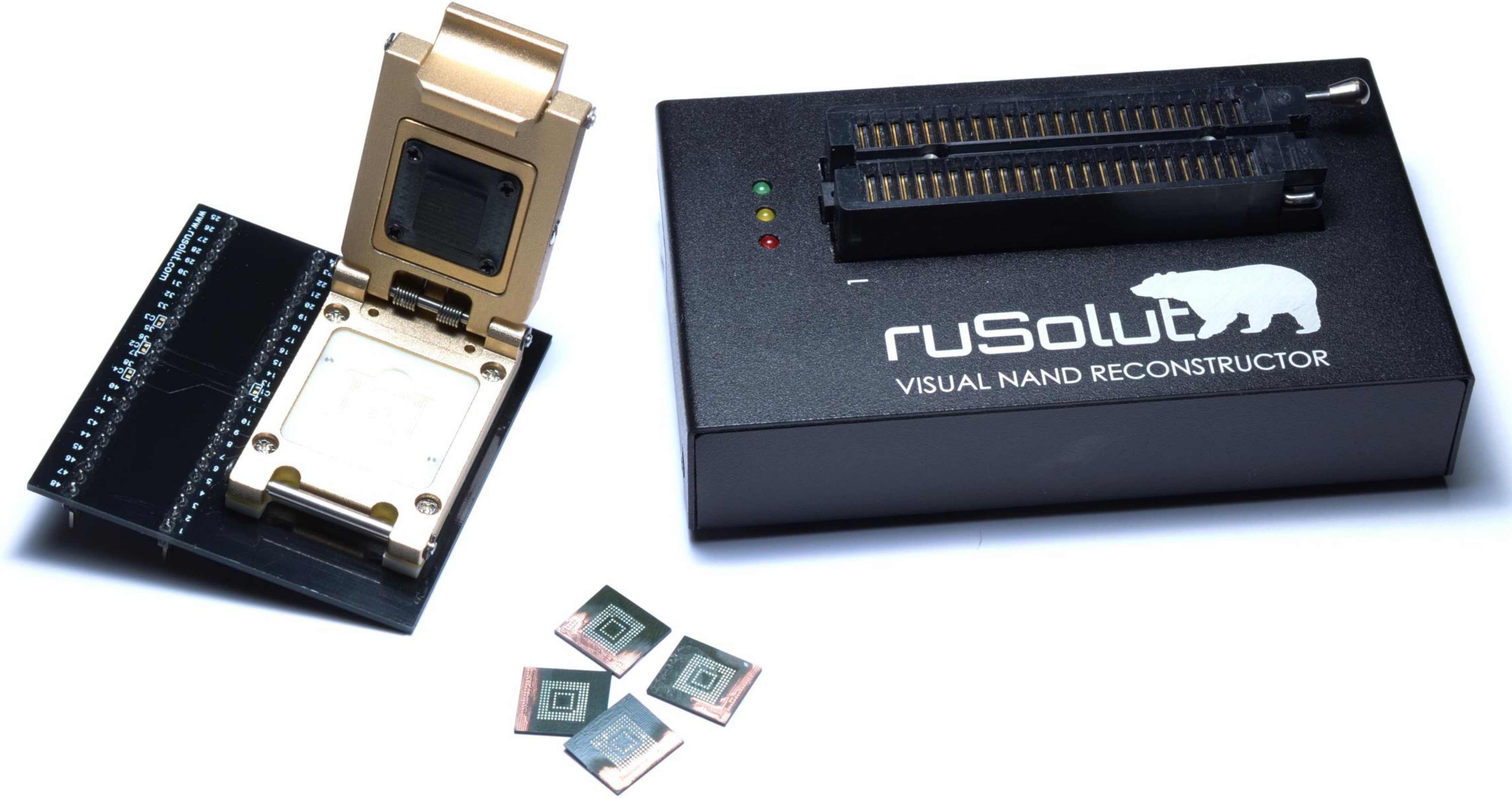
PROBLEMS WE HAD TO SOLVE TO TRANSFORM TECHNOLOGY INTO A TOOL

- UNKNOWN TECHNOLOGICAL NAND PINOUTS
- CONNECTING TO CHIPS
- NAND CONFIGURATIONS (EASY ONE)
- READ RETRY (DON’T MISS THIS PRESENTATION TODAY!)
- ADAPTIVE SCRAMBLING SCHEMES (NIGHTMARE)
- SCRAMBLED DA+SA+ECC (DON’T MISS THIS PRESENTATION TODAY!)
- PAGE BASED TRANSLATION ALGORITHMS ☹
- DEVELOPMENT OF SPECIAL SQLITE CARVER & FILE CARVER (DON’T MISS THESE PRESENTATIONS TODAY!)

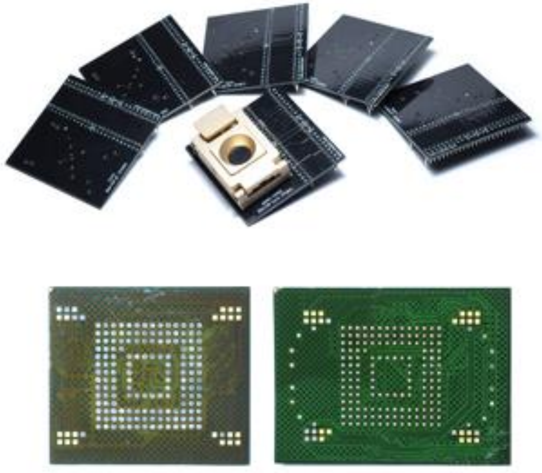
DIVERSITY OF DEVICES AND TECHNOLOGICAL PINOUTS

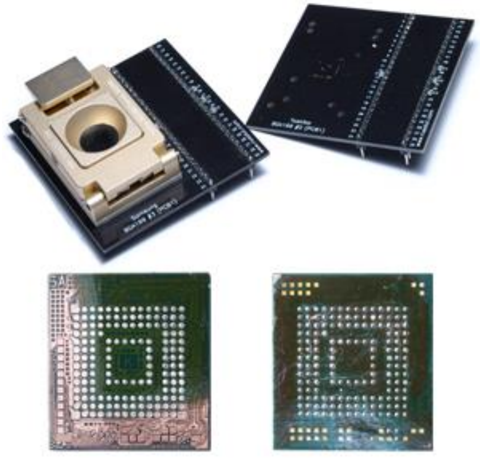


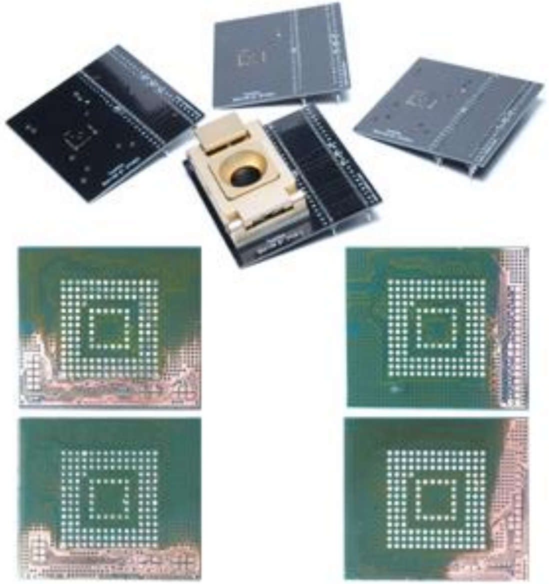
eMMC NAND RECONSTRUCTOR - HARDWARE

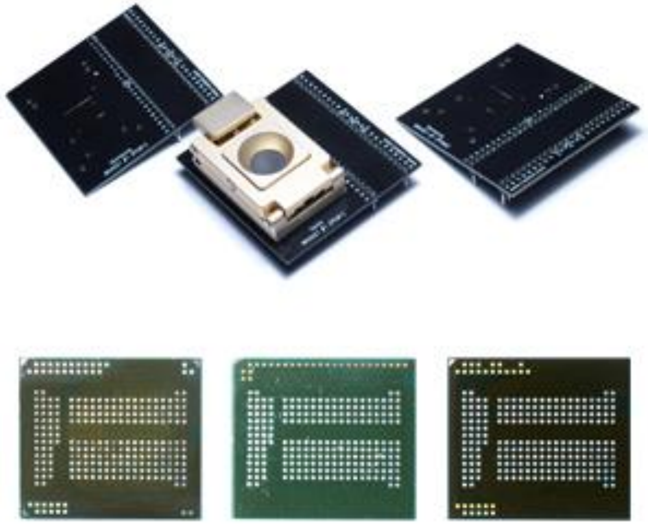


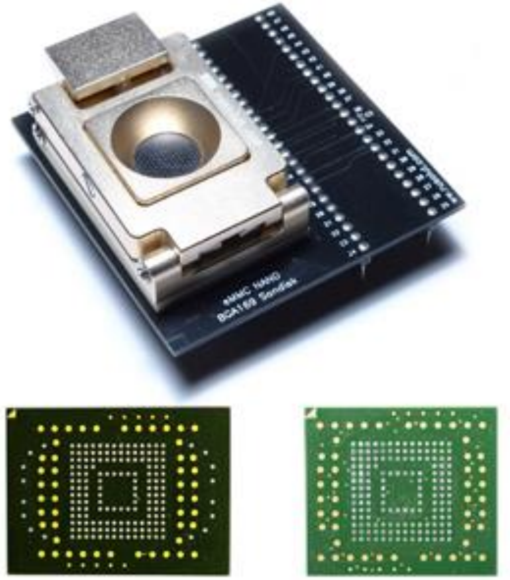
eMMC NAND RECONSTRUCTOR - ADAPTERS

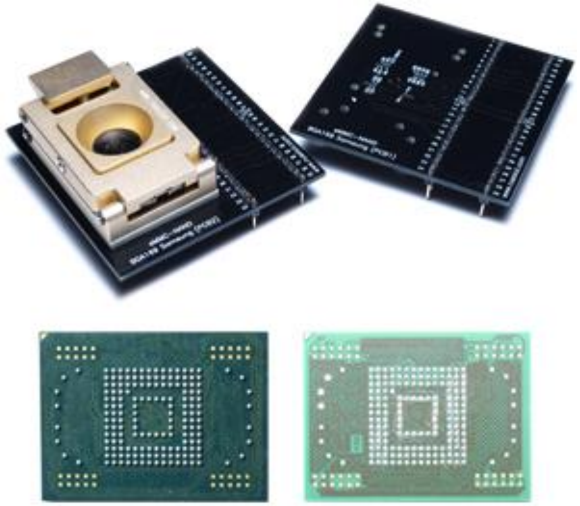


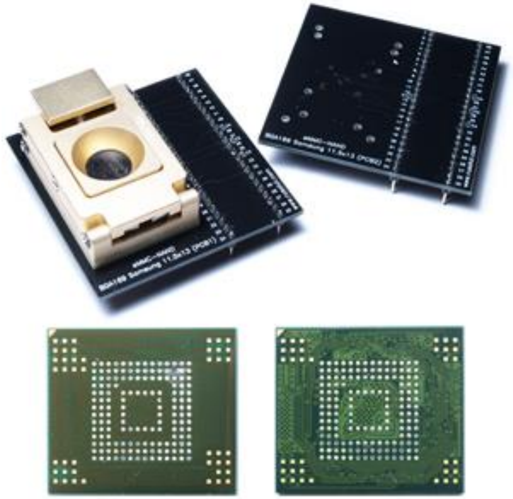






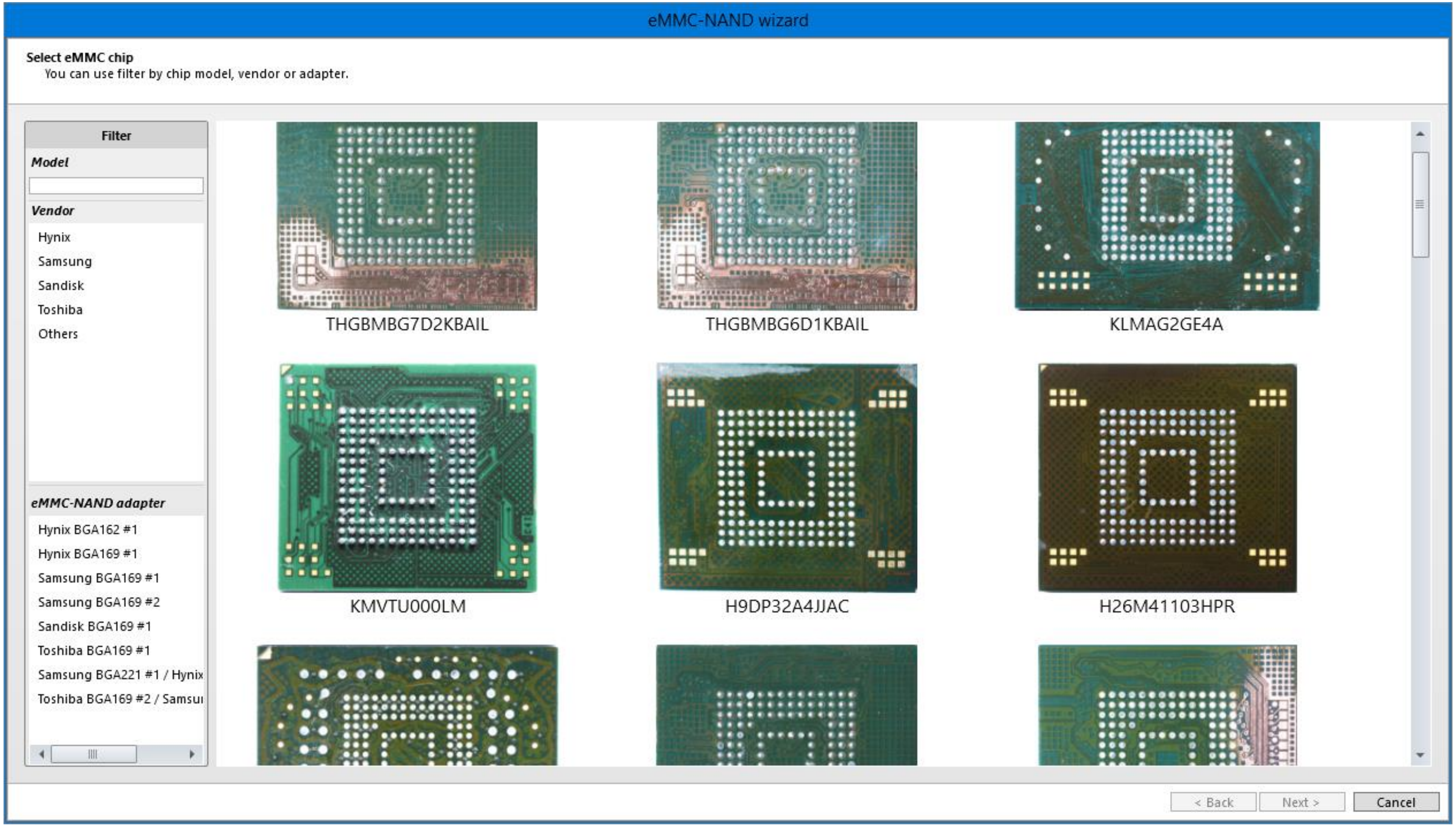






ruSolut

eMMC NAND RECONSTRUCTOR - SOFTWARE

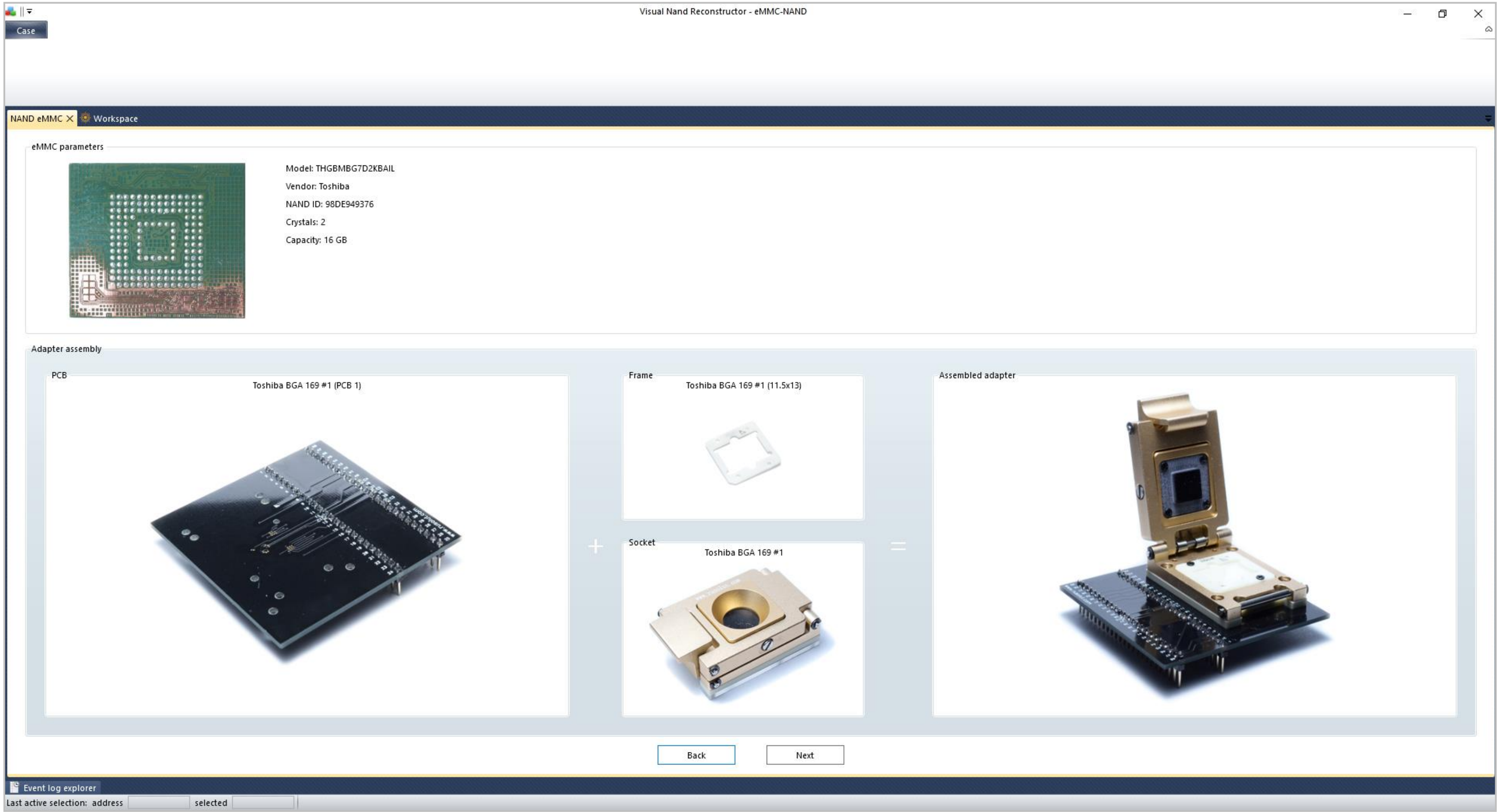


eMMC-NAND wizard

Select eMMC chip

You can use filter by chip model, vendor or adapter.

eMMC NAND RECONSTRUCTOR - SOFTWARE



Model: THGBMBG7D2KBAIL

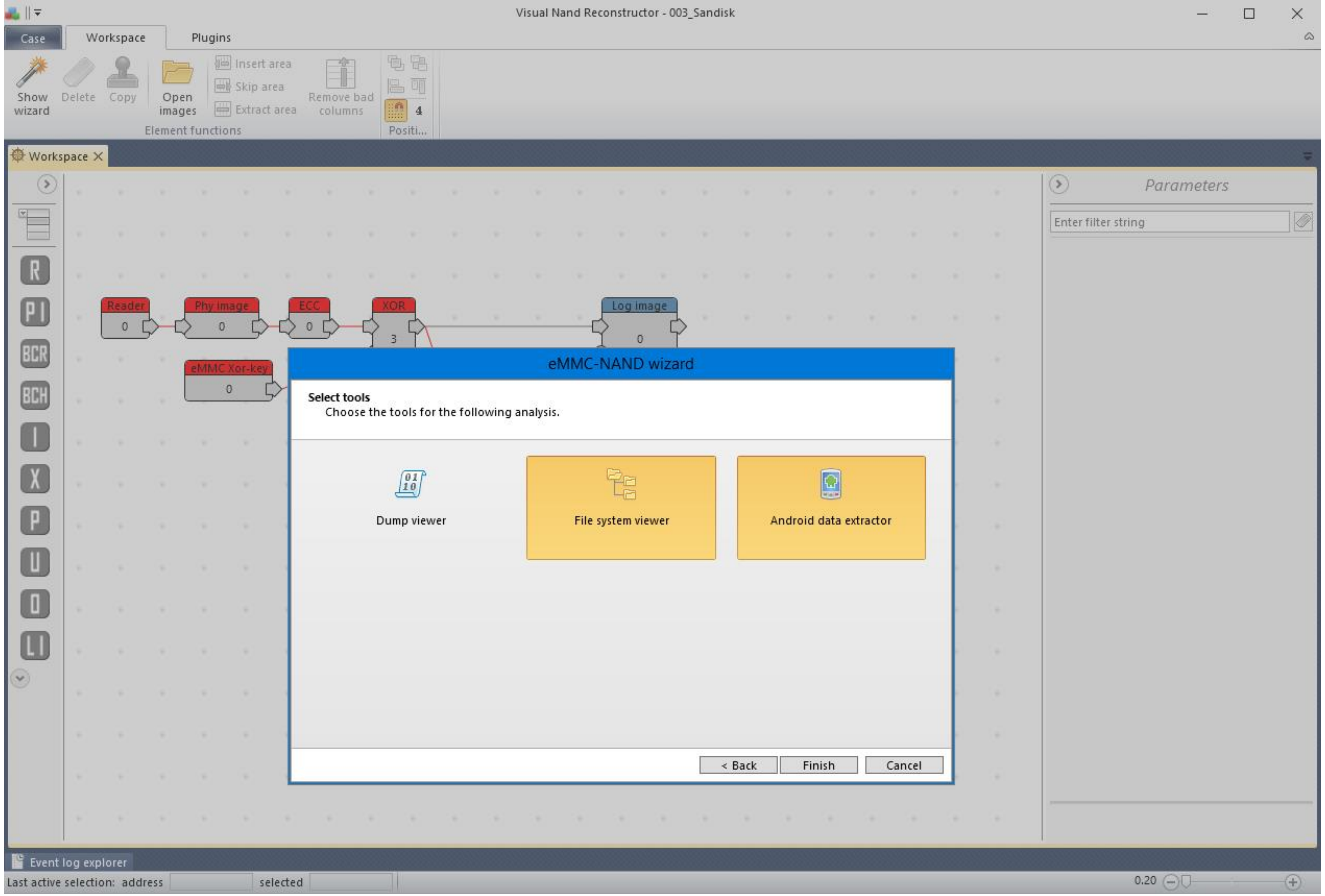
Vendor: Toshiba

NAND ID: 98DE949376

Crystals: 2

Capacity: 16 GB

AUTOMATIC CONTROLLER RECONSTRUCTION



Select tools

Choose the tools for the following analysis.

NOW LET’S TAKE A SHORT COFFEE BREAK AND MOVE FORWARD TO PRACTICAL PART

WE HAVE A QUICK 15-MIN WORKSHOP AREAS WHERE YOU CAN HAVE SOME CHAT WITH OUR ENGINEERS!