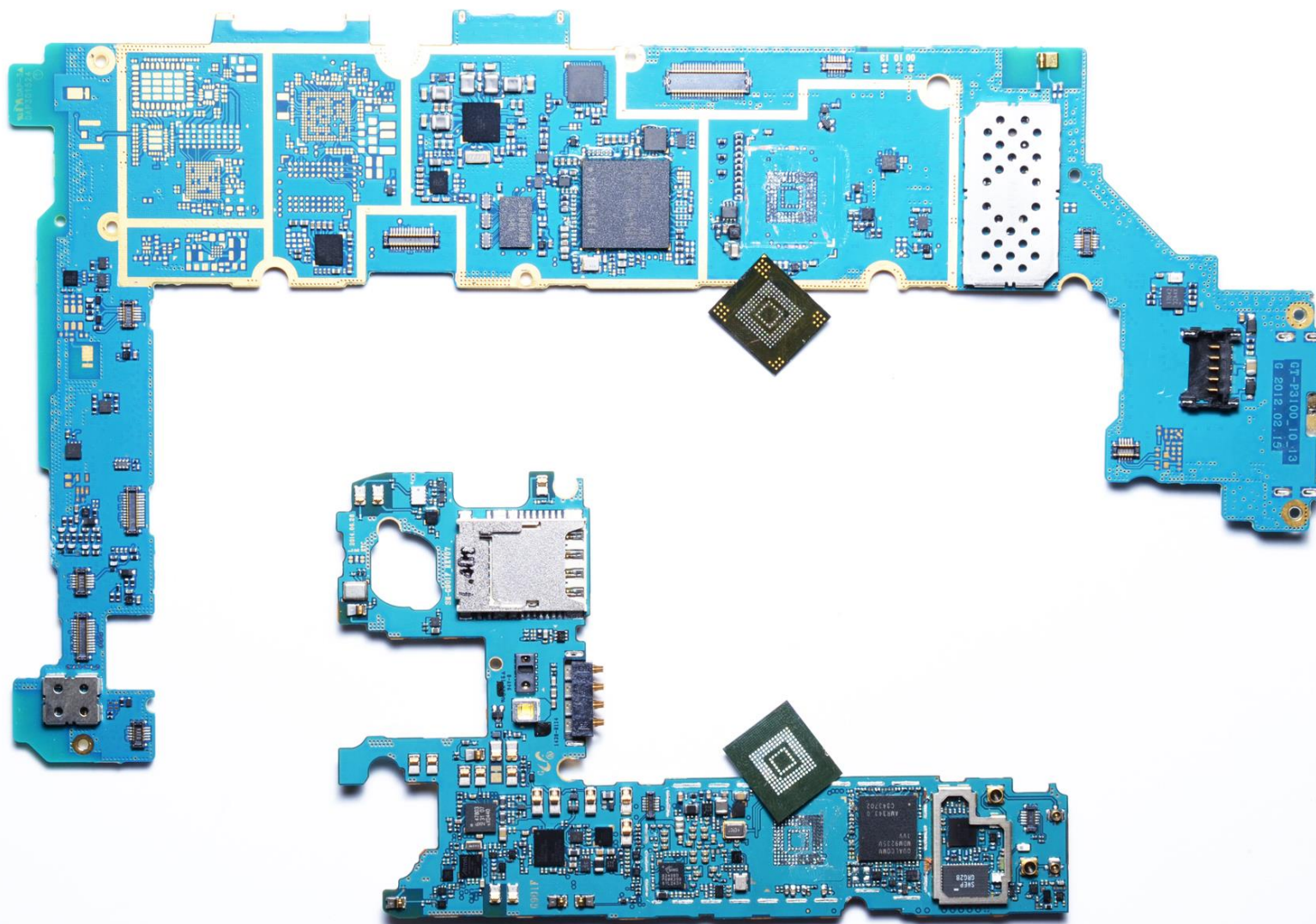


THE ULTIMATE CHIP-OFF MOBILE FORENSICS: DATA RESURRECTION FROM DEAD EMMC CHIPS

Rusolut

CHIP-OFF DATA RECOVERY FROM FLASH MEMORY DEVICES

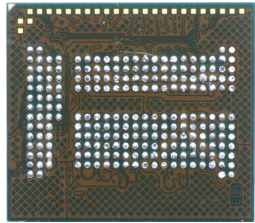


RAW NAND AND EMMC CHIPS USED IN PHONES AND OTHER DEVICES

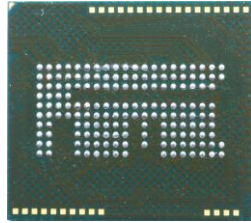
eMMC/eMCP

RAW NAND

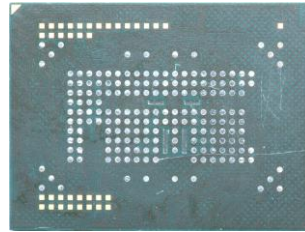
BGA221



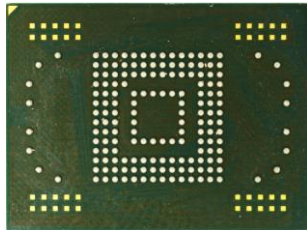
BGA162



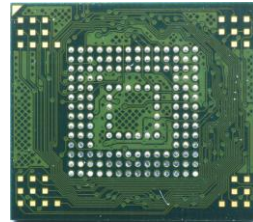
BGA186



BGA169 12x16



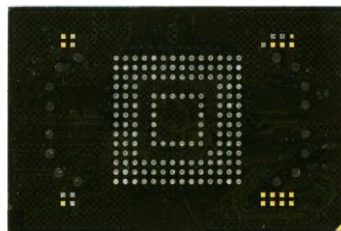
BGA153/169 11,5x13



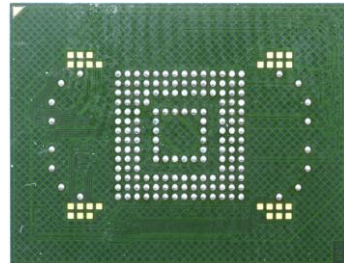
BGA153/169 10x11



BGA169 12x18



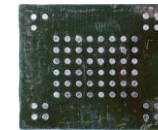
BGA169 14x18



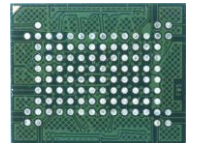
BGA137



BGA63

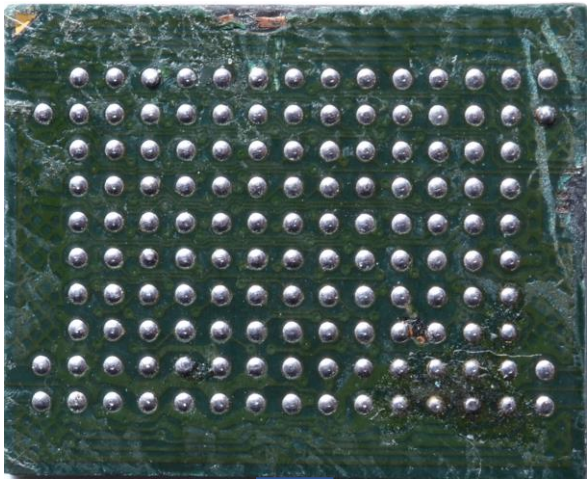


BGA107



EMMC vs RAW NAND CHIP-OFF DATA RECOVERY

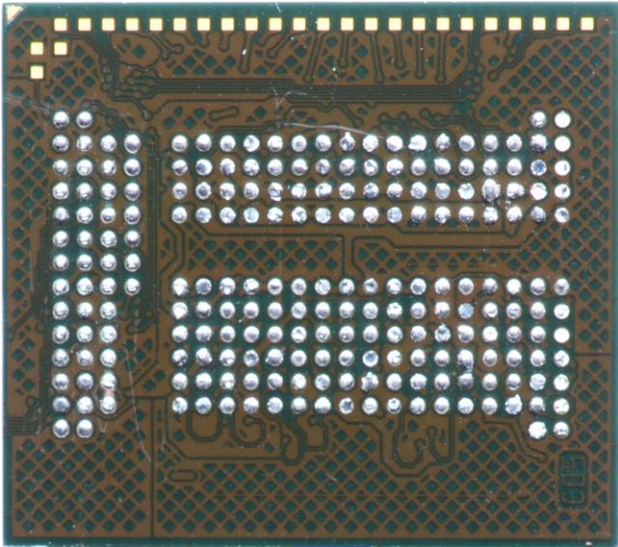
RAW NAND



READ

NAND protocol

eMMC/eMCP



READ

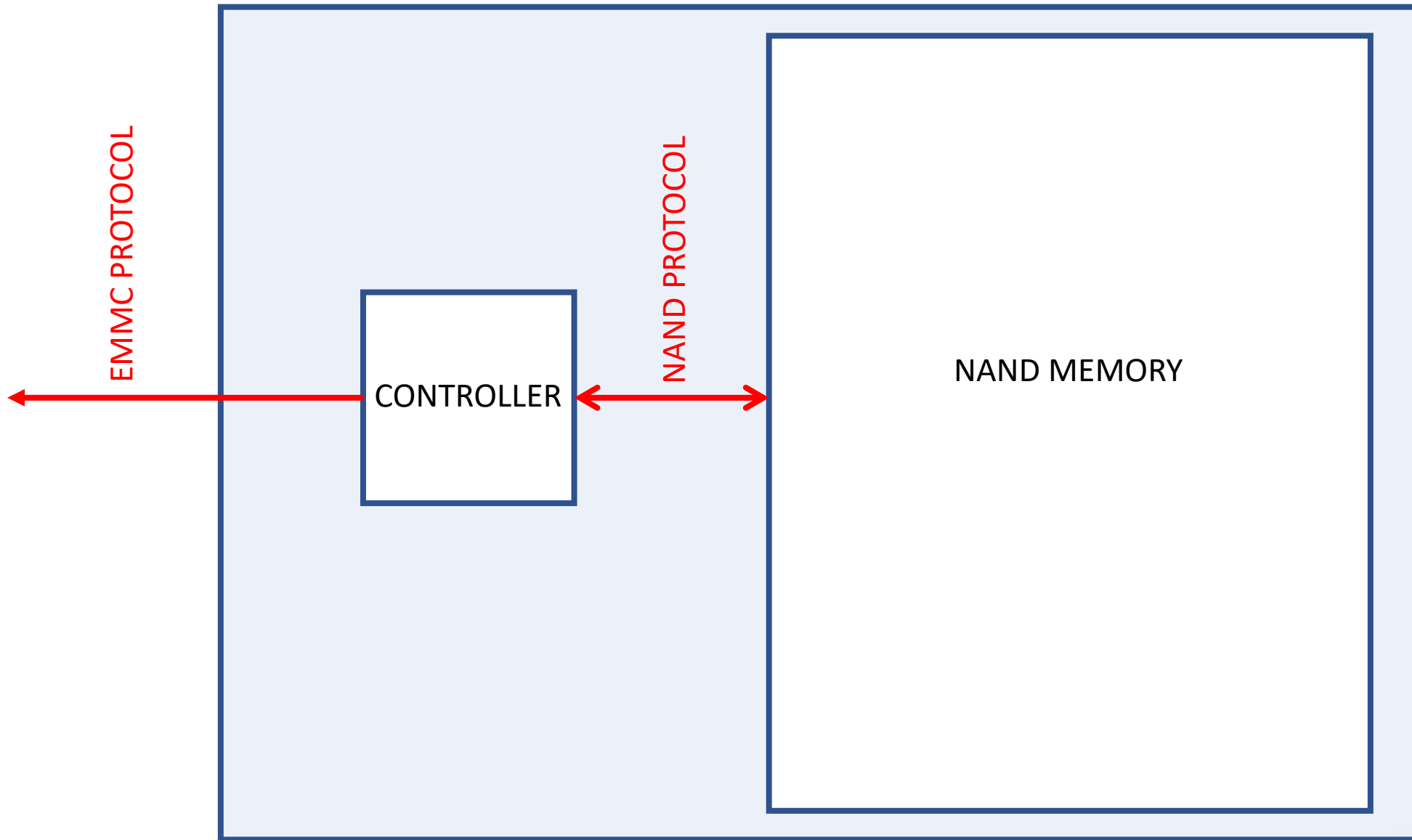
eMMC protocol

APPLICATIONS OF EMMC CHIPS

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

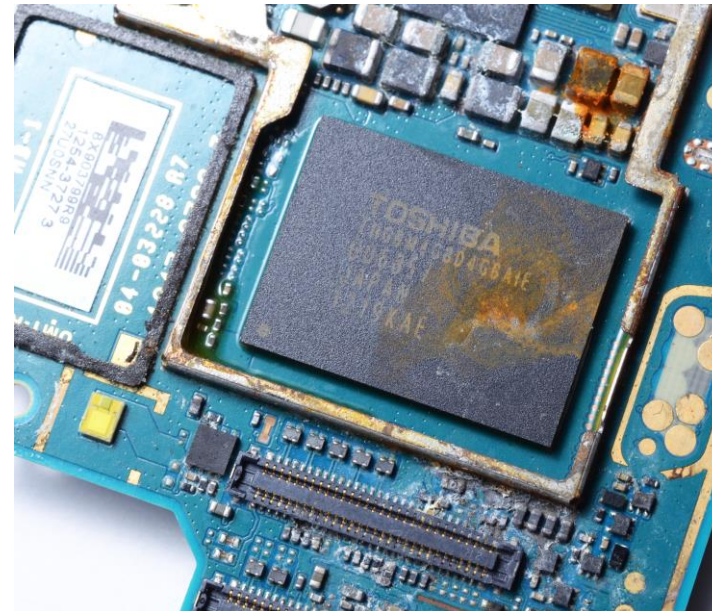
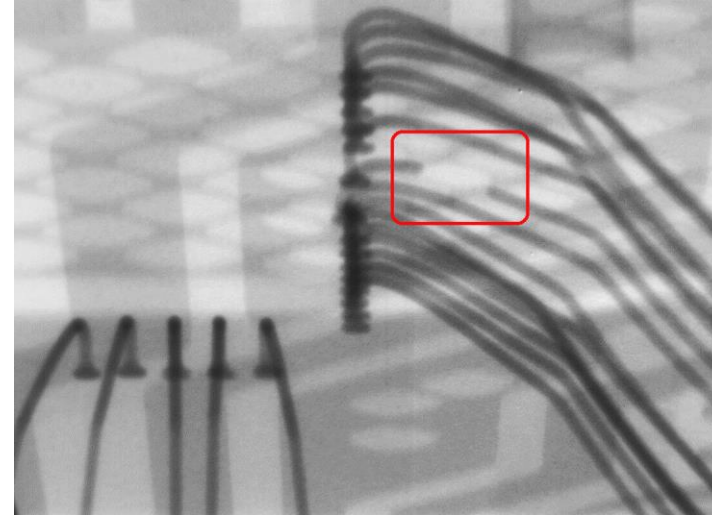
...AND MUCH MORE...

INSIDE EMMC



WHEN EMMC CHIP DAMAGE OCCURS

- 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



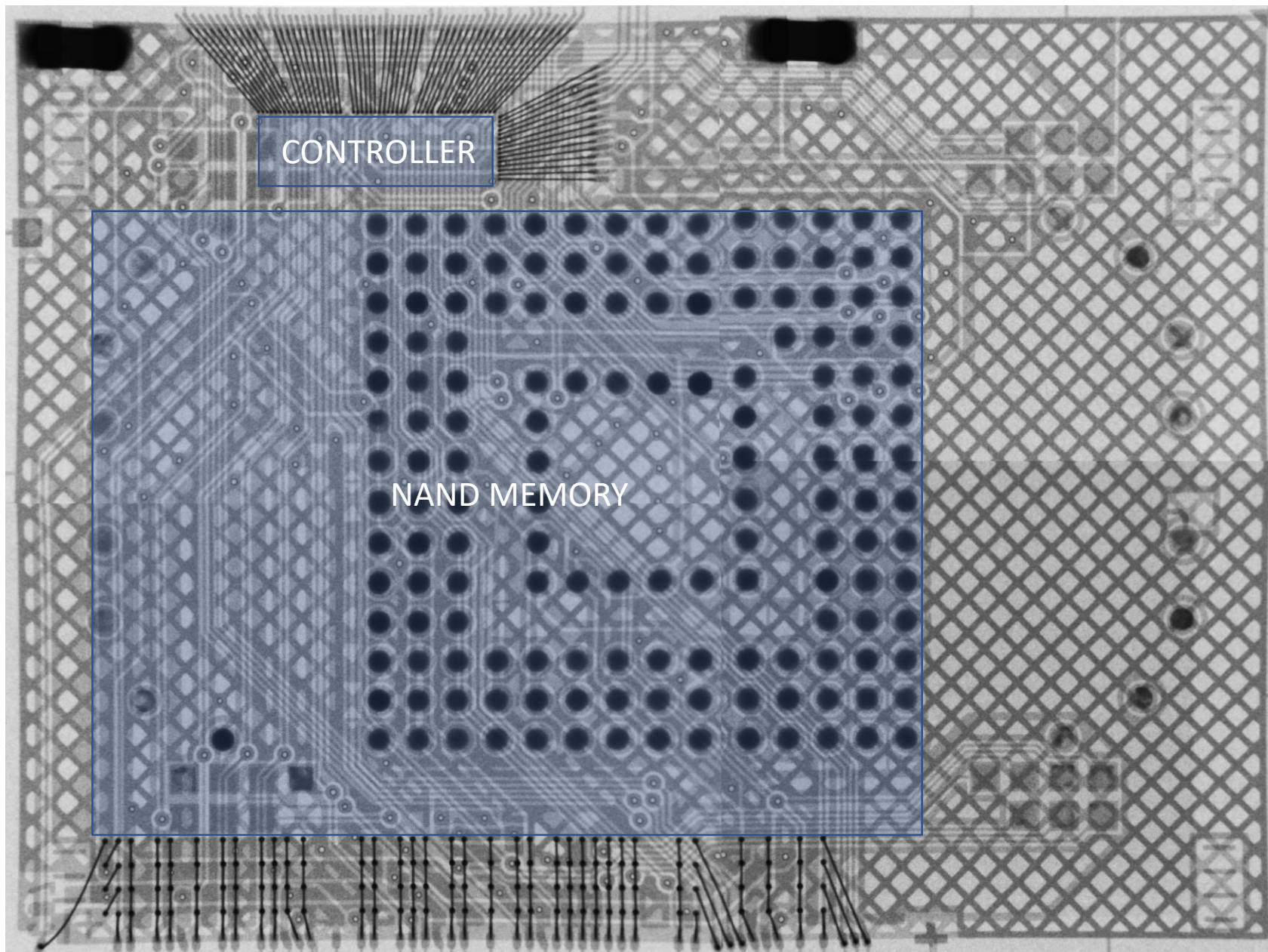
SYMPTOMS OF DAMAGED EMMC CHIPS

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

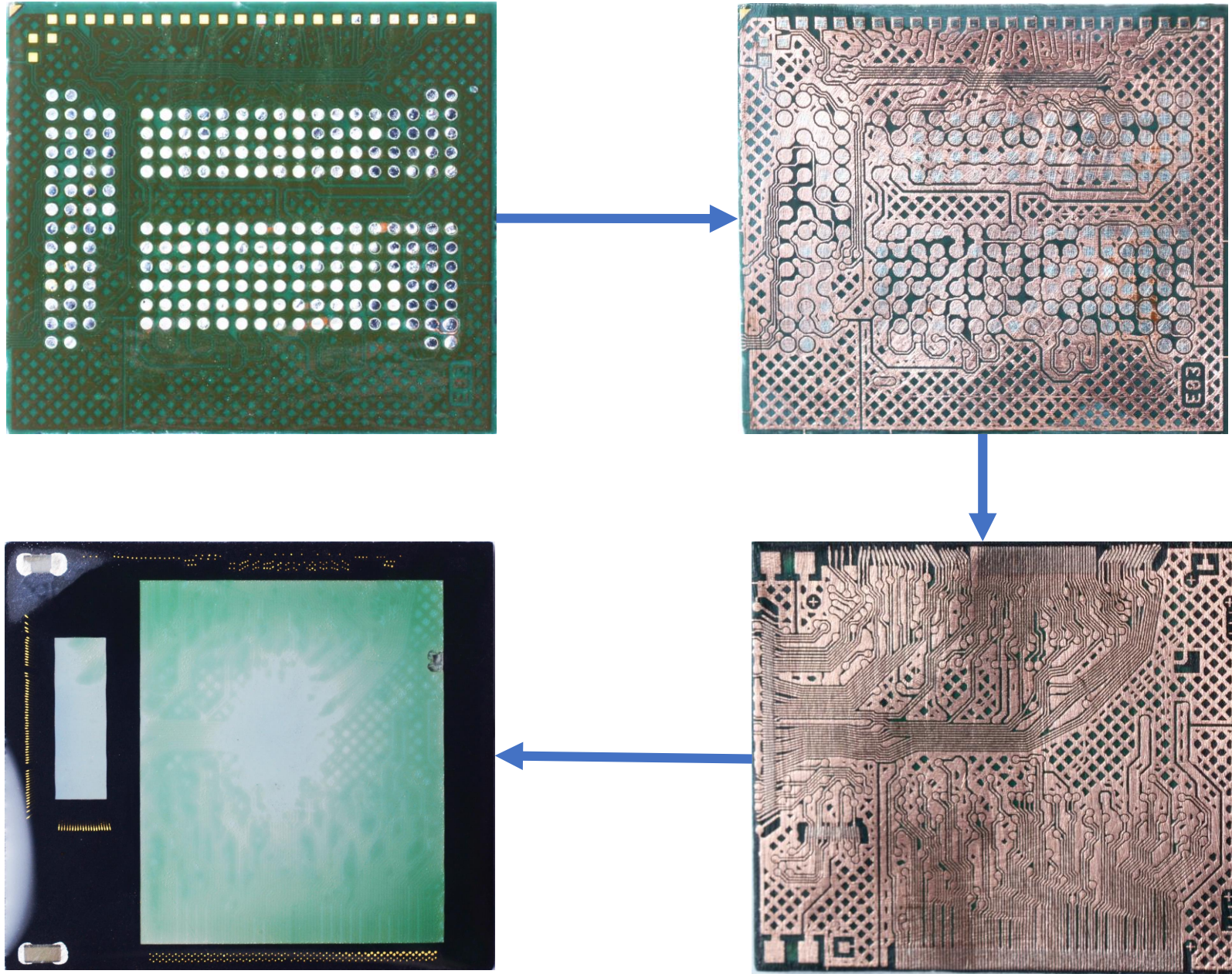


SO HOW TO EXTRACT THE DATA OUT OF DAMAGED EMMC CHIP?

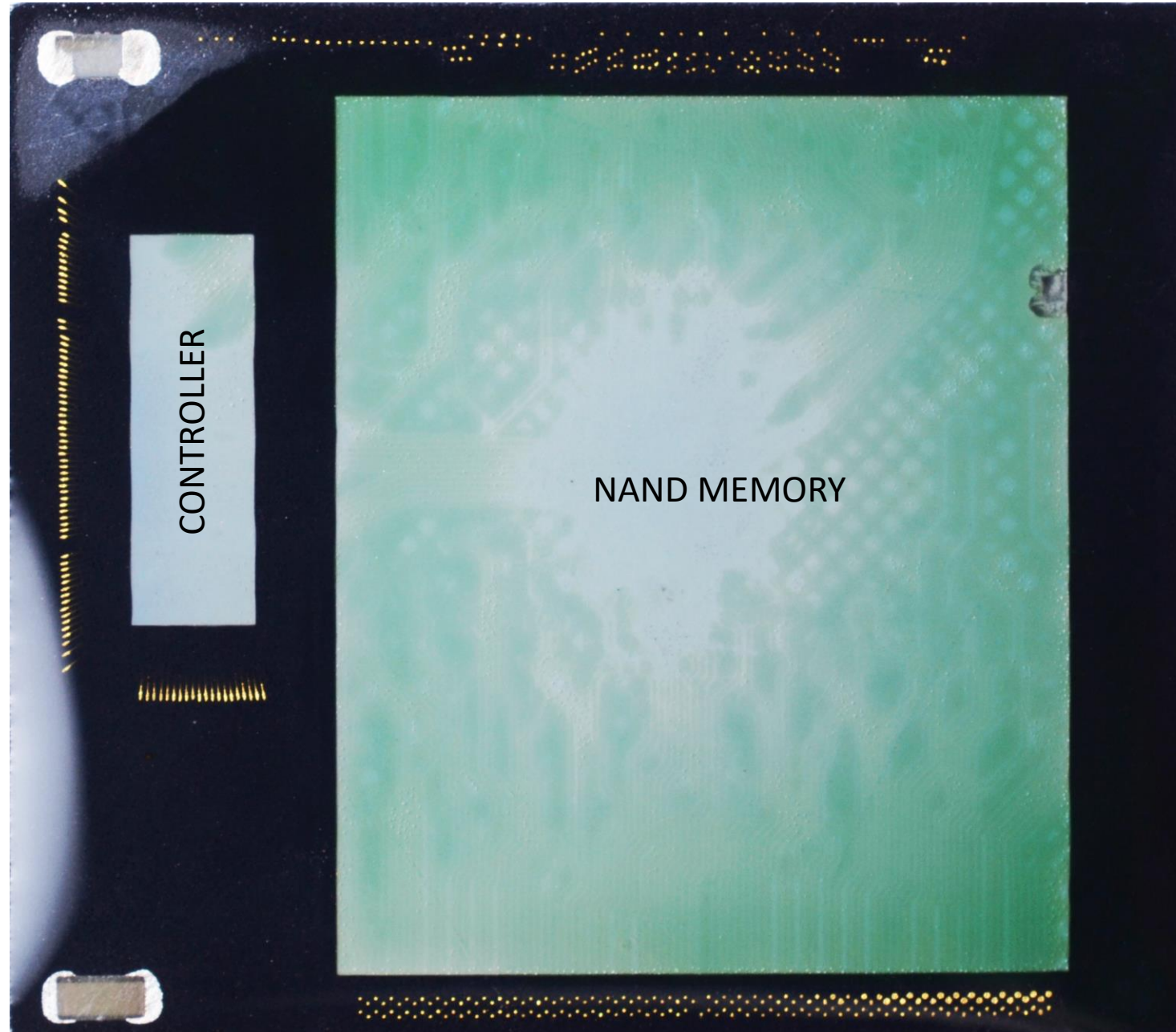
EMMC THROUGH XRAY



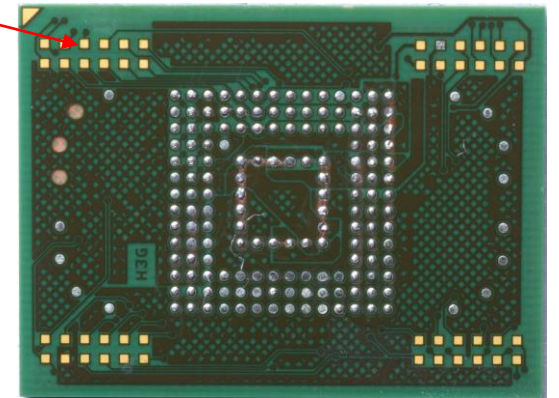
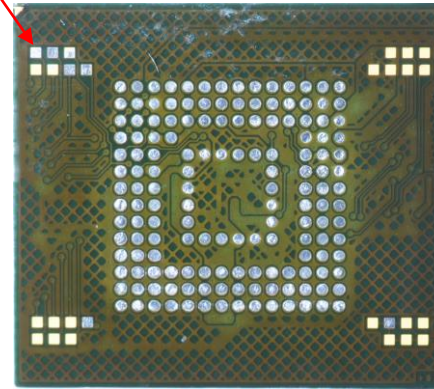
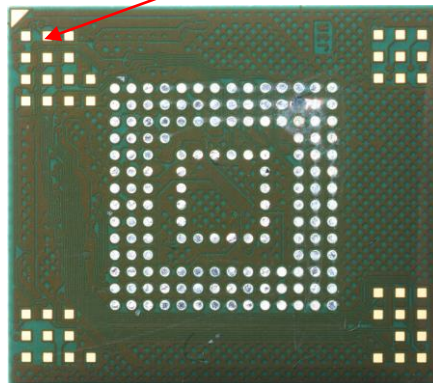
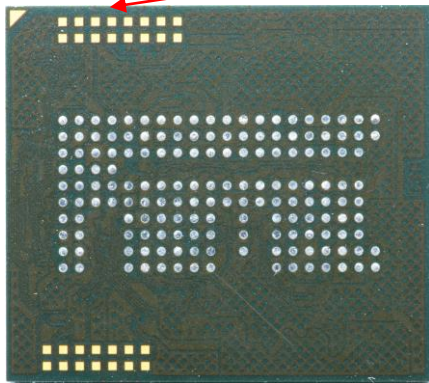
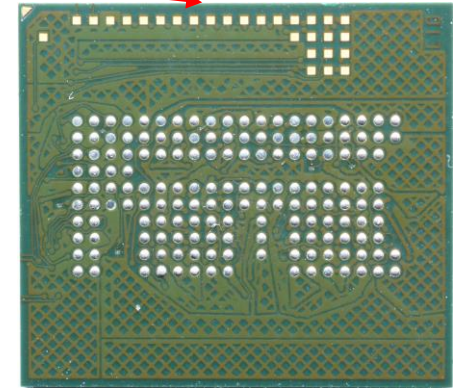
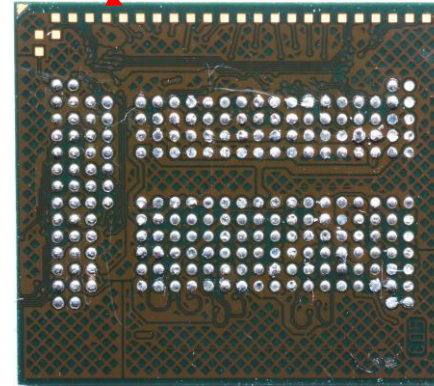
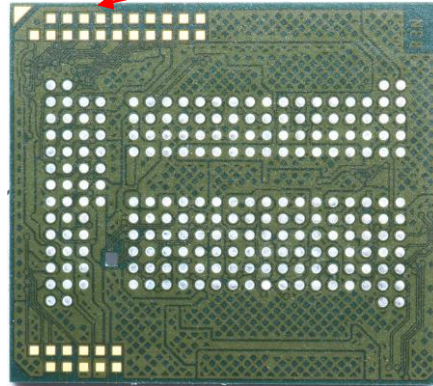
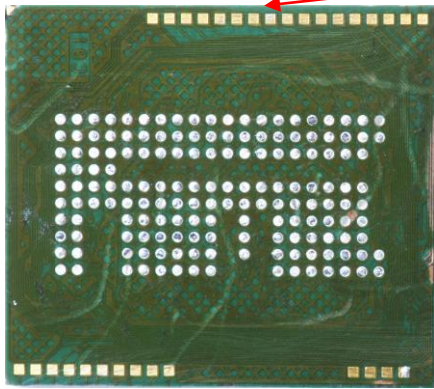
DELAYERED EMMC CHIP



EMMC CHIP STRUCTURE



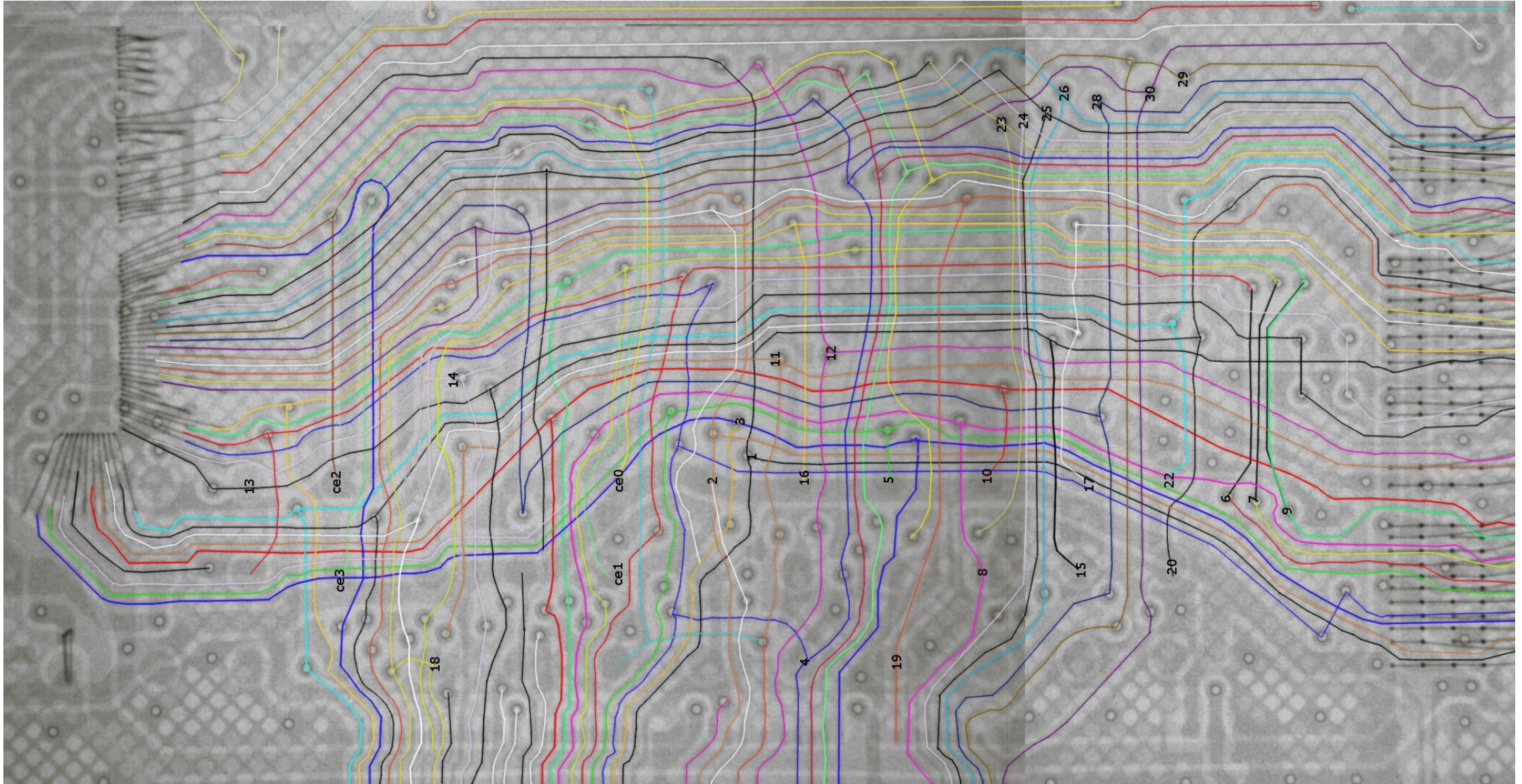
TECHNOLOGICAL PADS - NAND INTERFACE



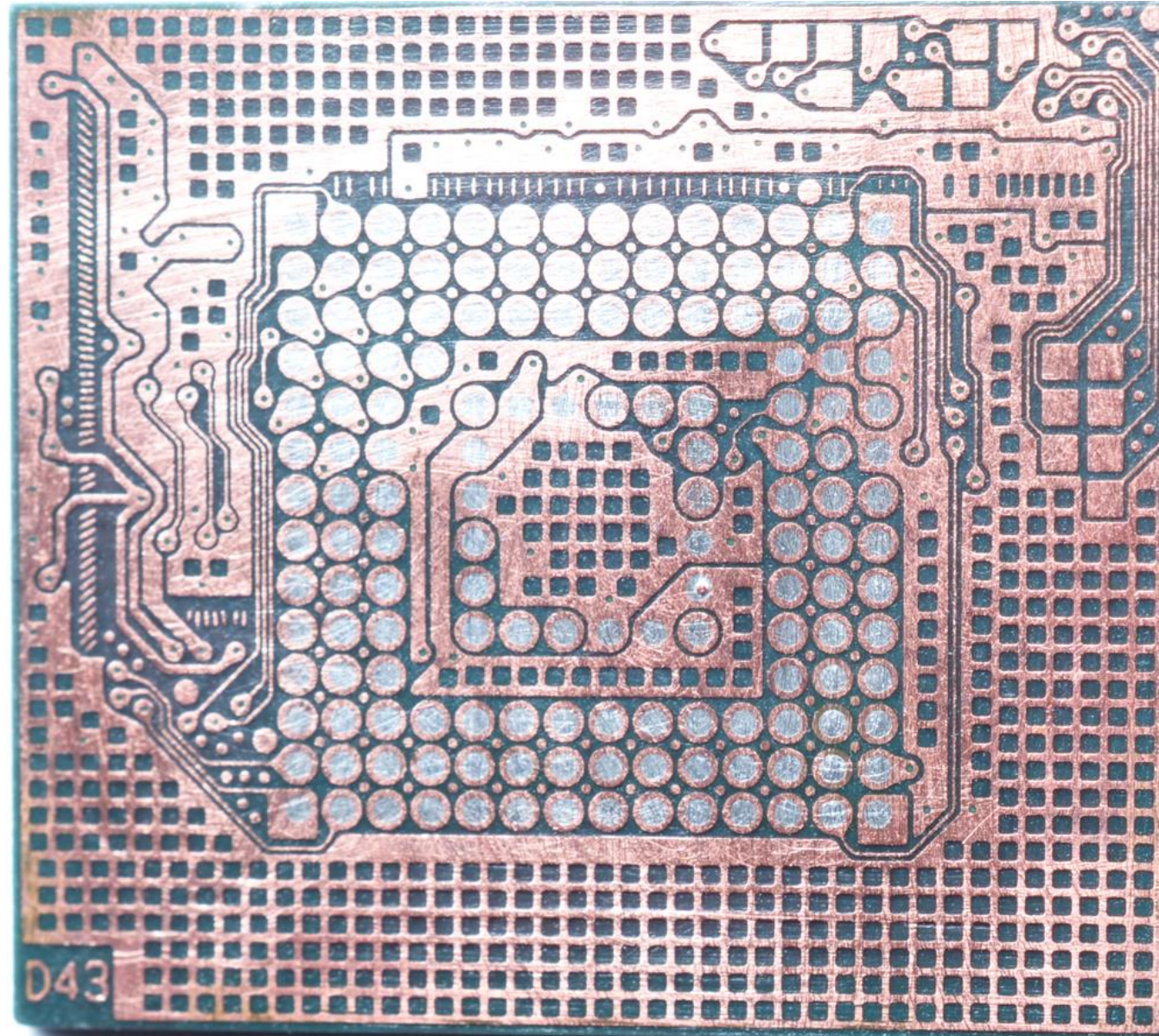
NAND PINOUT ANALYSIS

- 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 CONTROLLER AND NAND MEMORY

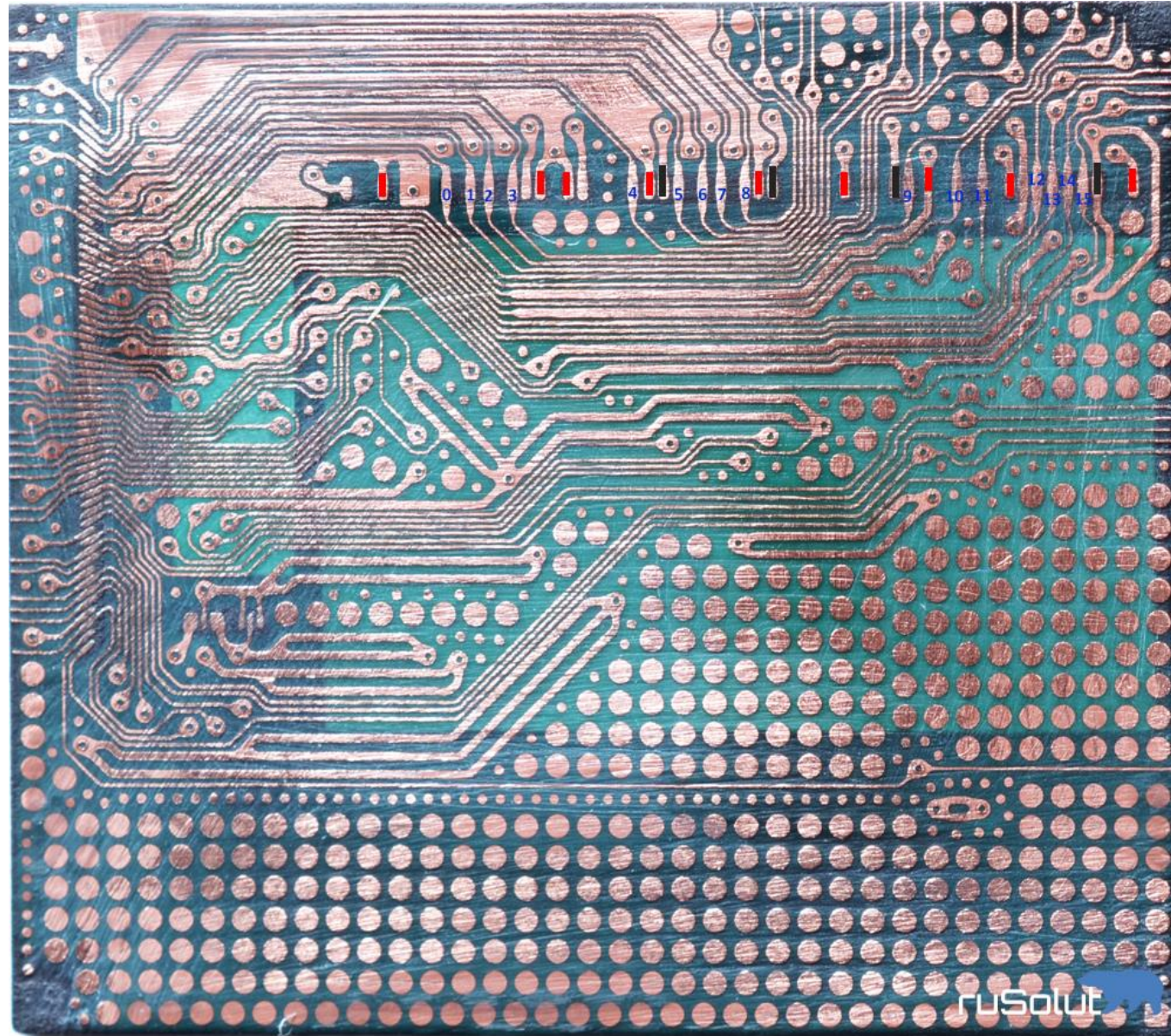
NAND PINOUT ANALYSIS. XRAY



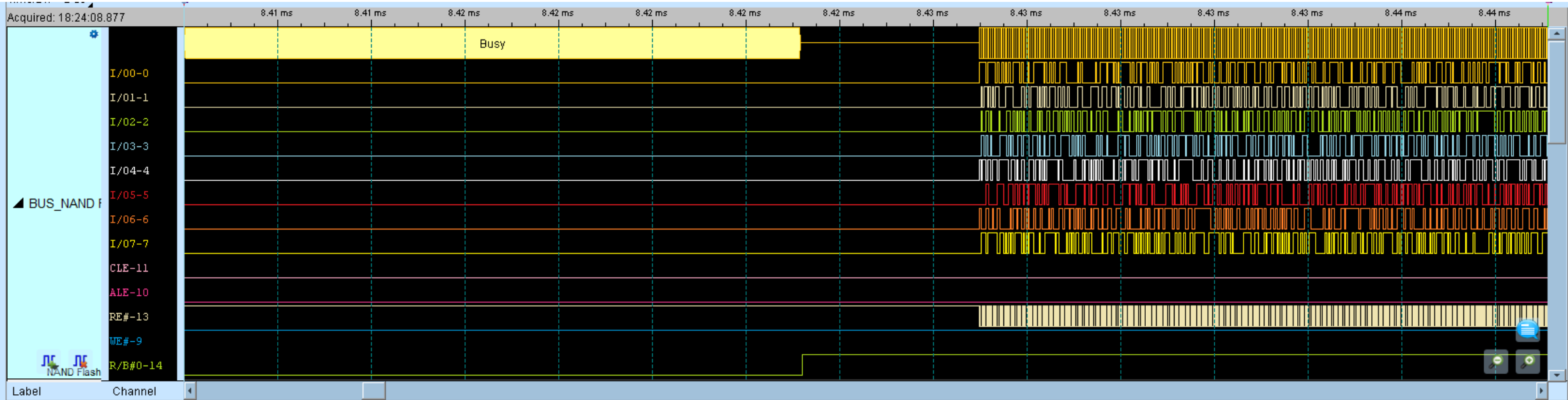
NAND PINOUT ANALYSIS. LAYER DISSECTION – LAYER 1 (TOP)



NAND PINOUT ANALYSIS. LAYER DISSECTION – LAYER 2 (INNER)

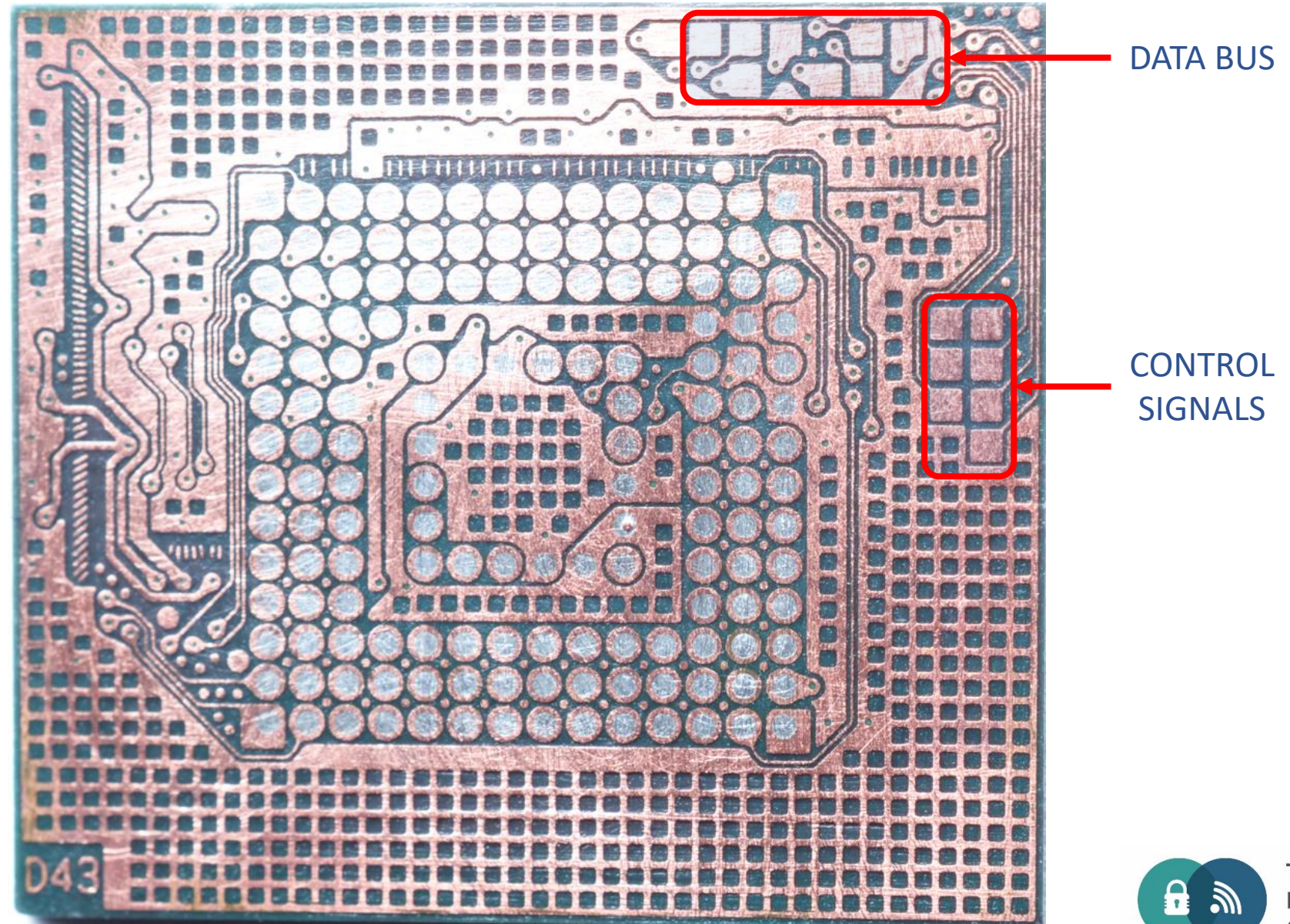


NAND PINOUT ANALYSIS. LOGIC ANALYZER



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	11.11155ms RESET(FF)											

NAND PINOUT



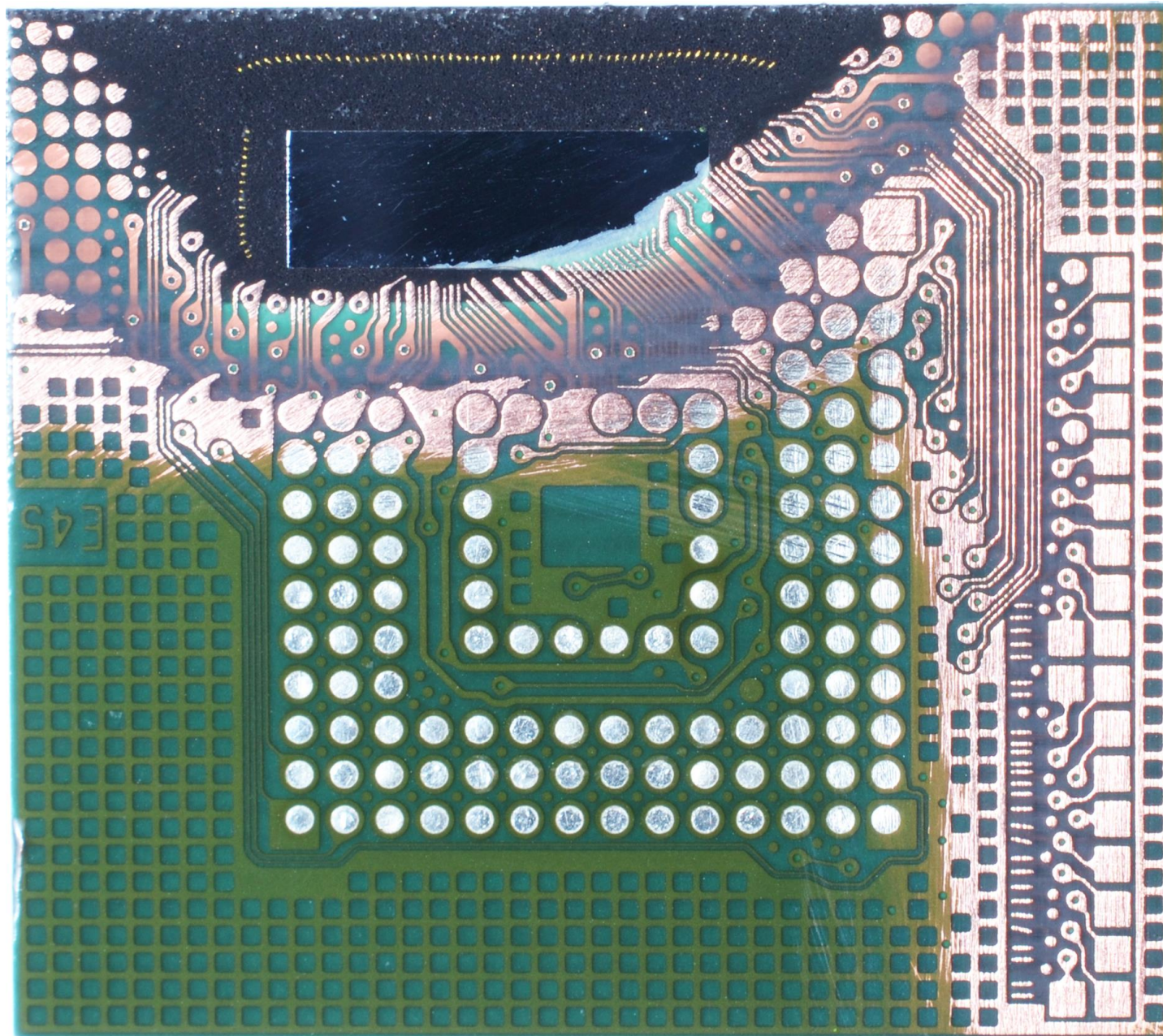
SCENARIOS OF FAILURE

NO SHORT CIRCUIT ~80-90%

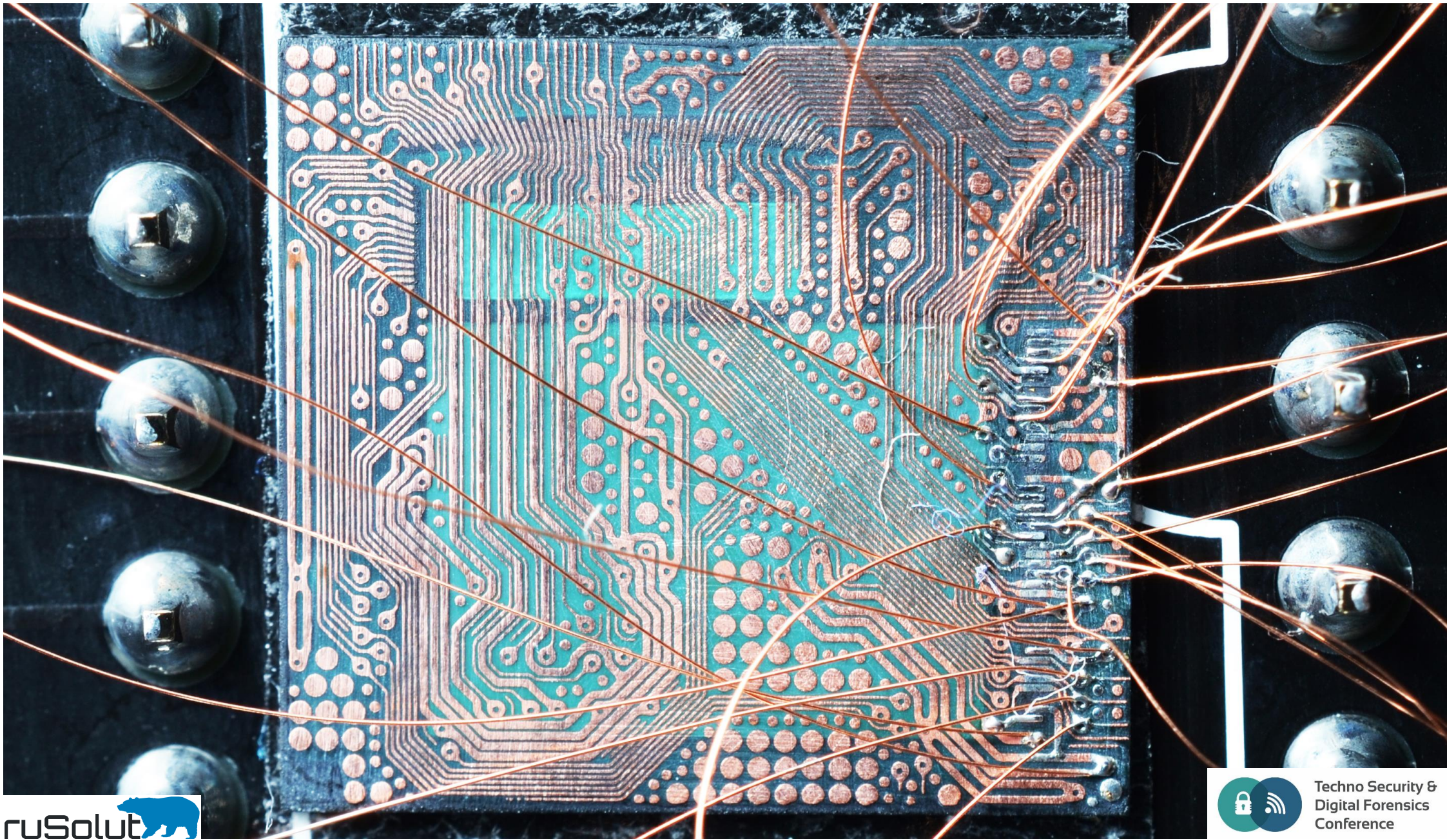
- FW CORRUPTION
- CONTROLLER DAMAGE DUE TO OVERHEAT
- WIRE BONDING DAMAGE
- UNKNOWN COTROLLER DAMAGES

SHORT CIRCUIT ~10-20%

SHORT CIRCUIT IN CONTROLLER. CONTROLLER DISCONNECTION. EASY CASE

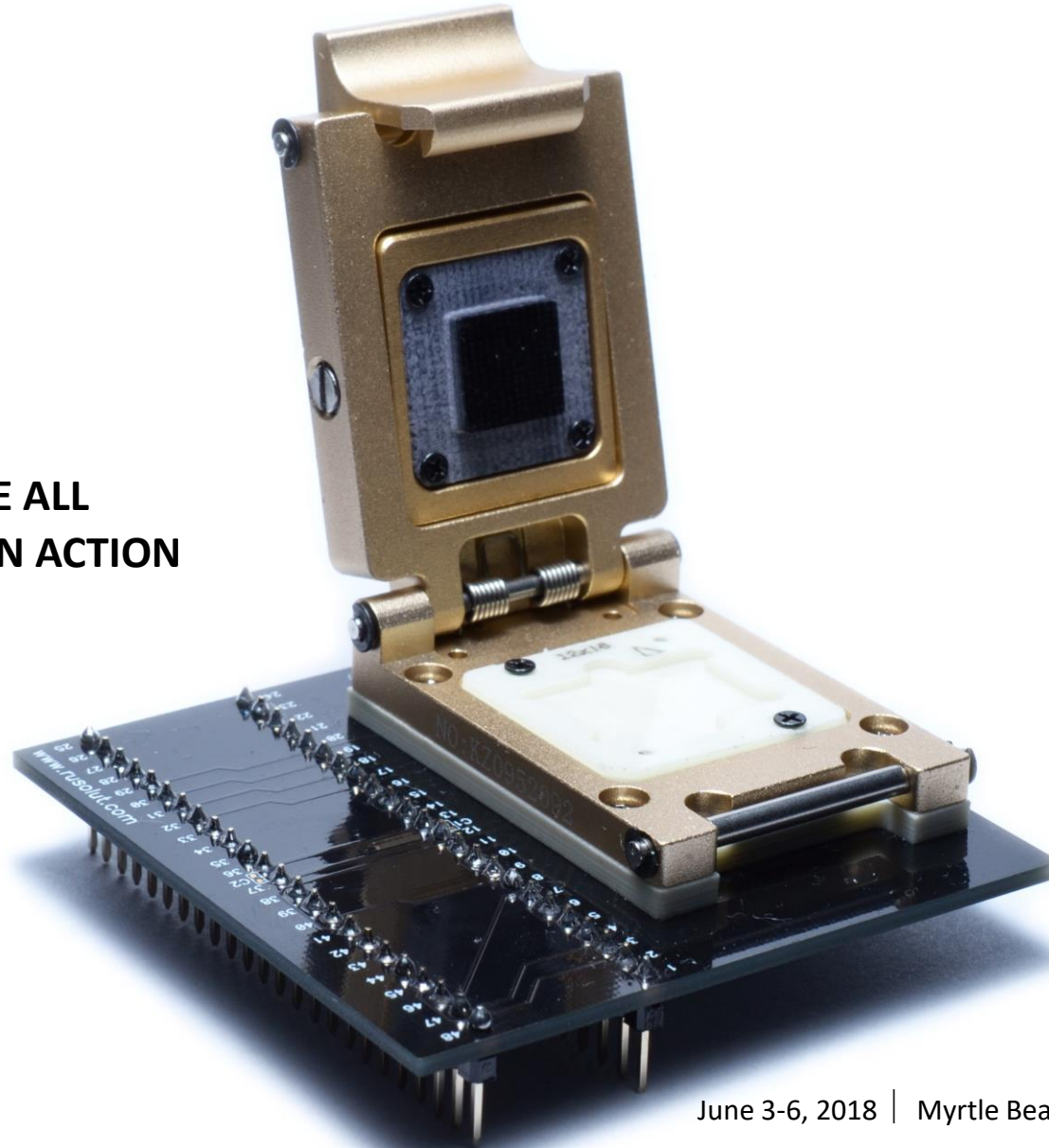


SHORT CIRCUIT IN CONTROLLER. CONNECTING TO SECOND LAYER OF PCB. HARD CASE



EMMC-NAND ADAPTERS

VISIT **BOOTH 108** TO SEE ALL
ADAPTERS AND TECHNOLOGY IN ACTION



CONNECT CHIP TO READER



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

Visual Nand Reconstructor - eMMC-NAND

Case

NAND eMMC X Workspace

Vendors

- Hynix
- Samsung
- Sandisk
- Toshiba
- Others

Find chip

THGBMBG7D2KBAIL

THGBMFG7C2LBAIL

THGBMBG6D1KBAIL

KLMAG2GE4A

KLM8G2FEJA

KMVTU000LM

H9DP32A4JJAC

H26M41103HPR

SDIN5C2-8G CHINA

TY90HH131517RA

THGBMBG7C2KBAIL

THGBMAG5A1JBAIL

eMMC-NAND adapters

- Hynix BGA 162 #1
- Hynix BGA 169 #1
- Samsung BGA 169 #1
- Samsung BGA 169 #2
- Sandisk BGA 169 #1
- Toshiba BGA 169 #1

selected

Techno Security & Digital Forensics Conference

ADAPTER ASSEMBLY

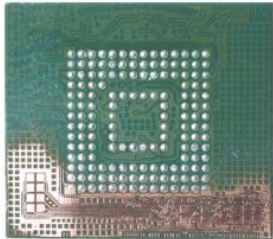
Visual Nand Reconstructor - eMMC-NAND

Case



NAND eMMC X Workspace

eMMC parameters



Model: THGBMBG7D2KBAIL
Vendor: Toshiba
NAND ID: 98DE949376
Crystals: 2
Capacity: 16 GB

Adapter assembly

PCB

Toshiba BGA 169 #1 (PCB 1)



Frame

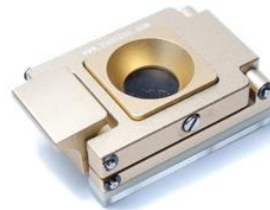
Toshiba BGA 169 #1 (11.5x13)



+

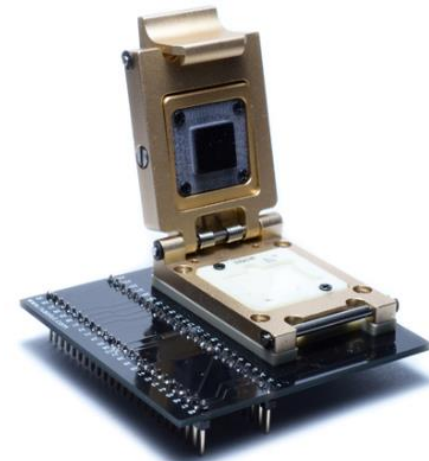
Socket

Toshiba BGA 169 #1



=

Assembled adapter



Back

Next

Event log

Last active selection

selected

RAW NAND PHYSICAL IMAGE EXTRACTION

Visual Nand R

Case Workspace Plugins

Delete Copy Open images Element functions Insert area Skip area Extract area Remove bad columns Positi...

Workspace X

Reader 0

Phy image Chip0_0_0

Phy image Chip1_0_0

Phy image Chip2_0_0

Phy image Chip3_0_0

15%

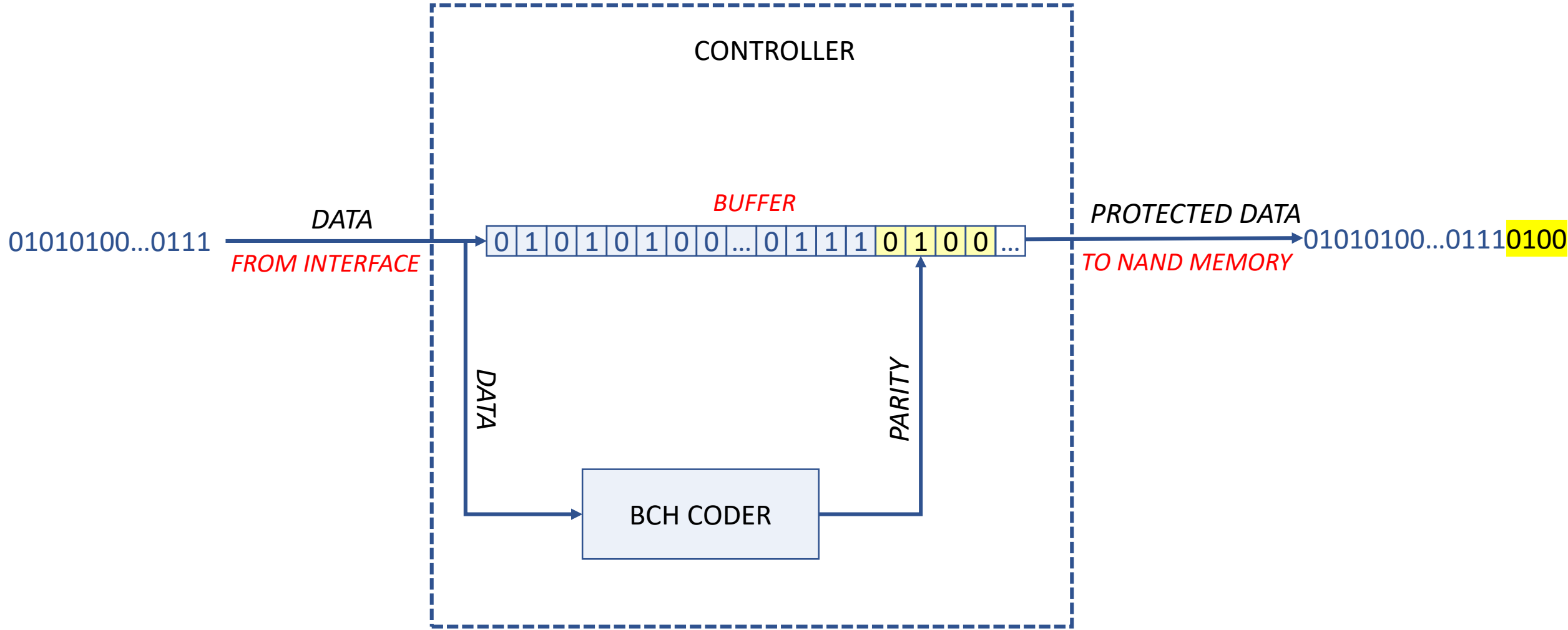
Reading dump from reader...

Chip: Chip0
Port: 0
Crystal: 0

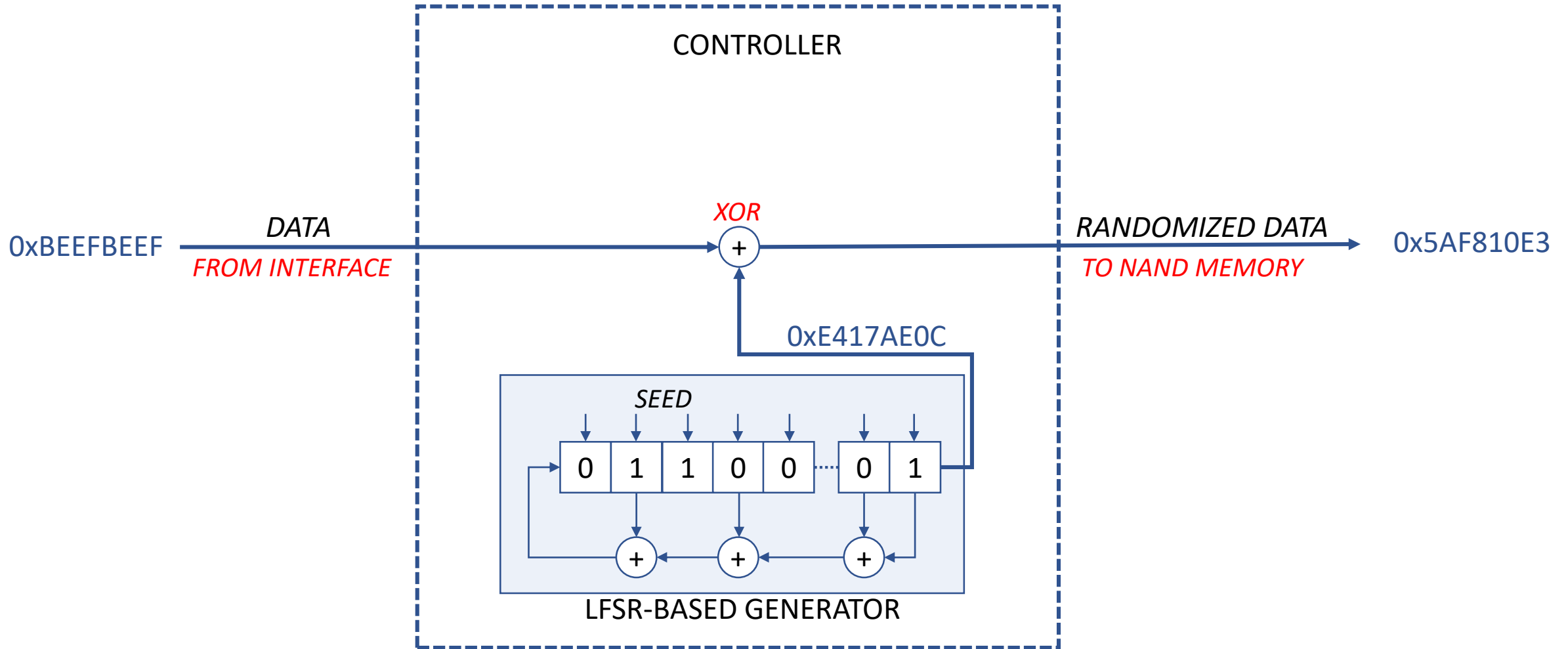
Cancel

R
PI
BCR
BCH
I
X
P
U
O
LI

ERROR CORRECTION CODES IN FLASH MEMORY

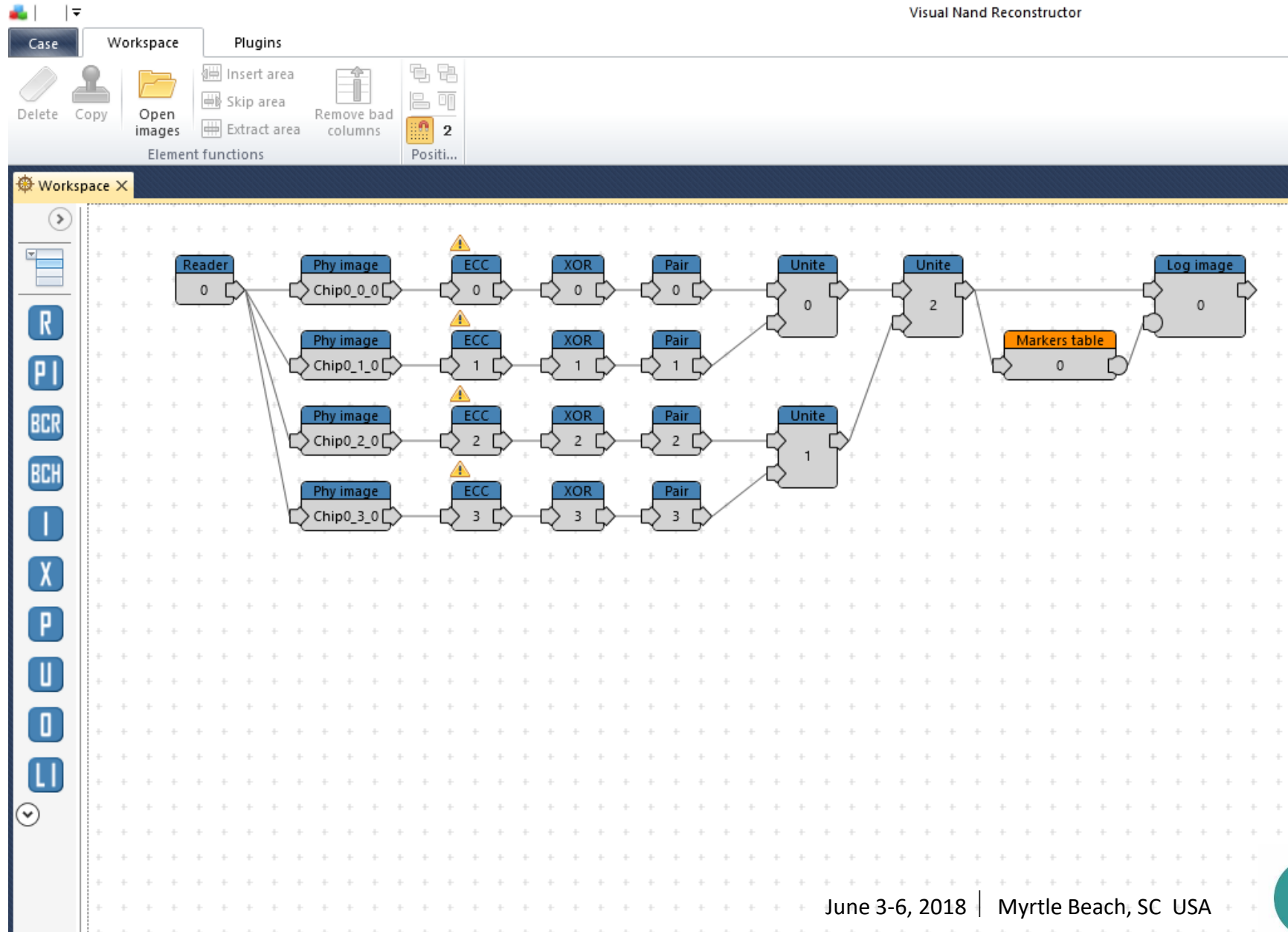


DATA SCRAMBLERS OF FLASH CONTROLLERS



LOGICAL IMAGE RECONSTRUCTION

Visual Nand Reconstructor



SQLITE CARVING AND DATA ANALYSIS

Visual Nand Reconstructor

Case Messages

Export Save Find Find next

Data extraction (Data area 0) Messages summary SMS carver Data area 0 Workspace

Messages (21)

	Group by: None		Type	Folder	Timestamp (UTC+0)	From	To	Message	Source
3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	SMS	Inbox	24/12/2013 16:50:41	+4850589		Zdrowia, szczęcia, pomyslnosci, nie polykaj z karpia osci, nie jedz bombek, Nie pal siana, jedz pierogi, lep balwana, a w sylwestra, pij do rana!!Zyczy Lukasz	Carver
4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	SMS	Sent	24/12/2013 16:42:21		+4866724	Dziękuję bardzo, oraz z mojej strony najserdeczniejsze życzenia:)	Carver
5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	SMS	Inbox	24/12/2013 16:50:41	+4850589		Zdrowia, szczęcia, pomyslnosci, nie polykaj z karpia osci, nie jedz bombek, nie pal siana, jedz pierogi, lep balwana, a w sylwestra, pij do rana!!Zyczy Lukasz	Carver
6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	SMS	Sent	24/12/2013 16:42:21		+4866724	Dziękuję bardzo, oraz z mojej strony najserdeczniejsze życzenia:)	Carver
7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	SMS	Inbox	24/12/2013 17:22:29	+48506463		Co nie zajechales?	Carver
8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	SMS	Sent	24/12/2013 16:42:21		+4866724	Dziękuję(bardzo, oraz z mojej strony najserdeczniejsze życzenia:)	Carver
9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	SMS	Inbox	24/12/2013 16:50:41	+4850589		Zdrowia, szczęcia, pomyslnosci, nie polykaj z karpia osci, nie jedz bombek, nie pal siana, jedz pierogi, lep balwana, a w sylwestra, pij do rana!!Zyczy Lukasz	Carver
10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	SMS	Inbox	24/12/2013 17:22:29	+40506463		Co nie zajechales?	Carver
11	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	SMS	Inbox	24/12/2013 16:50:41	+4850589		Zdrowia, szczęcia, pomyslnosci, nie polykaj z karpia osci, nie jedz bombek, nie pal siana, jedz pierogi, lep balwana, a w sylwestRa, pij do rana!!Zyczy Lukasz	Carver
12	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	SMS	Sent	24/12/2013 17:23:03		+4850646	Zadzwonie za 10 minut jakoś	Carver
13	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	SMS	Inbox	24/12/2013 16:50:41	+4870589		Zdrowia, szczęcia, pomyslnosci, nie xolykaj z karpia osci, nie jedz bombek, nie pal siana, jedz pierogi, lep balwana, a w sylwestra, pij do rana!!Zyczy Lukasz	Carver
14	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	SMS	Inbox	24/12/2013 17:31:14	+4850646		Co nie zajechales?	Carver
15	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	SMS	Inbox	24/12/2013 16:50:41	+4850589		Zdrowia, szczęcia, pomyslnosci, nie polykaj z karpia osci, nie jedz bombek, nie pal siana, jedz pierogi, lep balwana, a w sylwestra, pij do rana!!Zyczy Lukasz	Carver
16	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	SMS	Sent	24/12/2013 16:42:21		+4866724	Dziękuję bardzo, oraz z mojej strony najserdeczniejsze życzenia:)	Carver
17	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	SMS	Inbox	24/12/2013 17:23:25	+4850646		Ok	Carver
18	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	SMS	Inbox	18/01/2014 13:22:04	+4850589		Zdrowia, szczęcia, pomyslnosci, nie polykaj z karpia osci, nie jedz bombek, nie pal siana, jedz pierogi, lep balwana, a w sylwestra, pij do rana!!Zyczy Lukasz	

Position 1 from 21

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

More details here:

https://www.flashmemorysummit.com/English/Collaterals/Proceedings/2017/20170808_S102A_Sheremetov.pdf

Shortlink: <https://goo.gl/g84gkJ>

VISIT OUR **BOOTH 108** TO SEE NEW TOOL UNVEIL AND TECHNOLOGY IN WORK



THANK YOU



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

June 3-6, 2018 | Myrtle Beach, SC USA



Techno Security &
Digital Forensics
Conference

OUR PARTNERS IN USA



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