



black hat[®]
EUROPE 2020

DECEMBER 9-10
BRIEFINGS

A New Hope: The One Last Chance to Save Your SSD Data

#BHEU @BLACKHATEVENTS

About us

- **Kwonyoup Kim, Founder, CEO of SNT Works Inc.**
- **Seungjoon Lee, Senior Researcher of SNT Works Inc.**

- **SNT Works Inc.**
 - **Specialized in Security Analysis on Embedded Systems**
 - ✓ **Reverse Engineering for Security Evaluation, Assessment**
 - ✓ **Offensive Security for Embedded Devices**
 - ✓ **Digital Forensics for Embedded Devices**
 - ✓ **Side Channel Attack & Fault Injection Attack with Reverse Engineering**
 - ✓ **Patent infringement Investigation**



SNTWORKS

Introduction

SSD Forensics : Myths and Reality

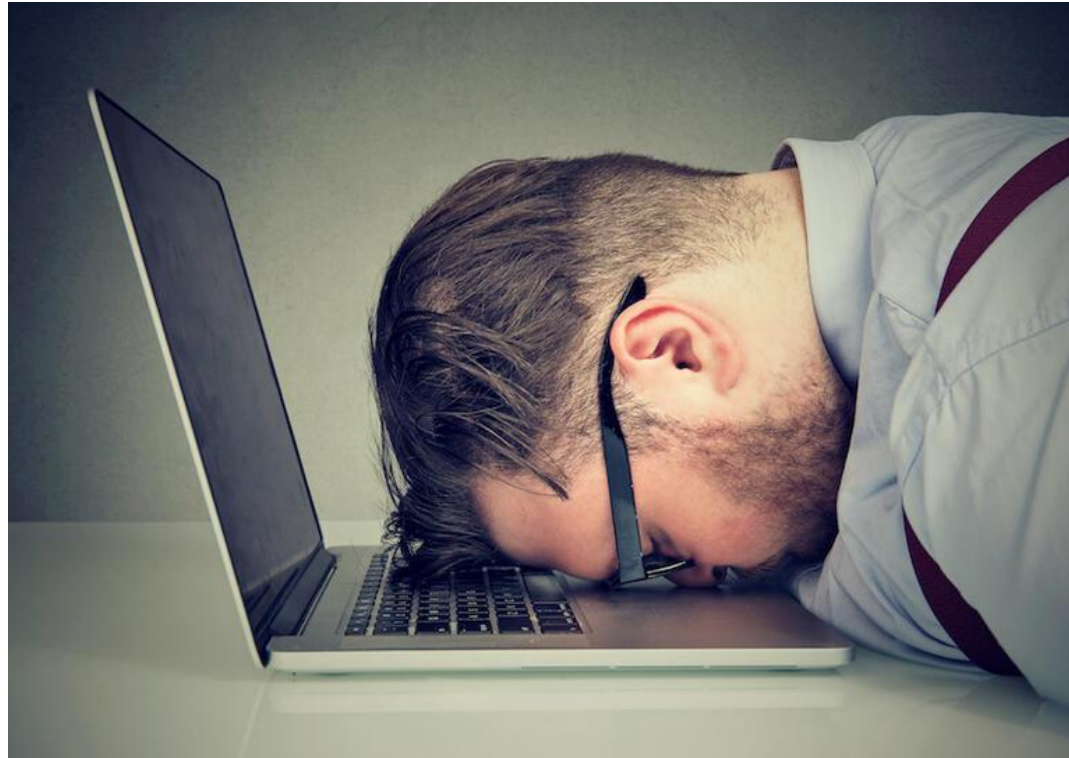
SSD Forensics : Myths and Reality

- **SSD Forensics Issues : Perfectly(Secure) Erase**
 - **Can SSD data be completely erased?**



SSD Forensics : Myths and Reality

- **SSD Forensics : Cannot Recovery Data**
 - **Can't we recover previous data from SSDs?**



SSD Forensics : Myths and Reality

▪ **Current status of SSD Forensics**

- **SSD Controller information is not disclosed**
- **Private SSD internal algorithm information**
- **Lack of SSD Physical Data collection tools (including data reconstruction function)**
- **Lack of SSD Physical Data recovery tools**

▪ **Our Challenges**

- **Build an environment to analyze the internal operation of Commercial SSDs**
- **Tracing the process of writing, reading and erasing SSD data**
- **SSD physical data collection**
- **Check and try SSD data recovery conditions**

SSD Firmware Reversing

Background

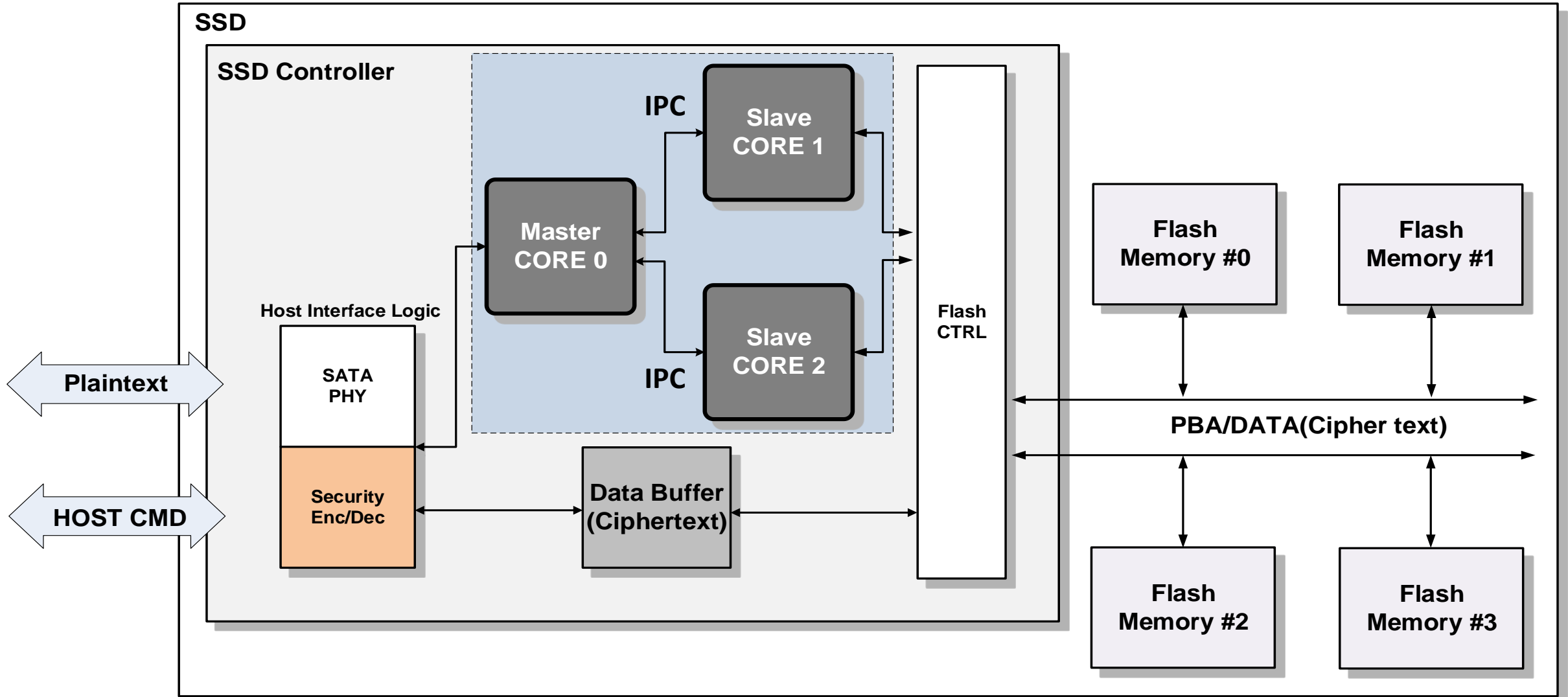
Why Commercial SSDs Reversing is Hard?

- **SSD Manufacturers**
do not divulge information.
- **SSD Controller manufacturers**
also do not divulge information.
- **They protect their**
implementation details to
protect their technologies.
- **No standards**



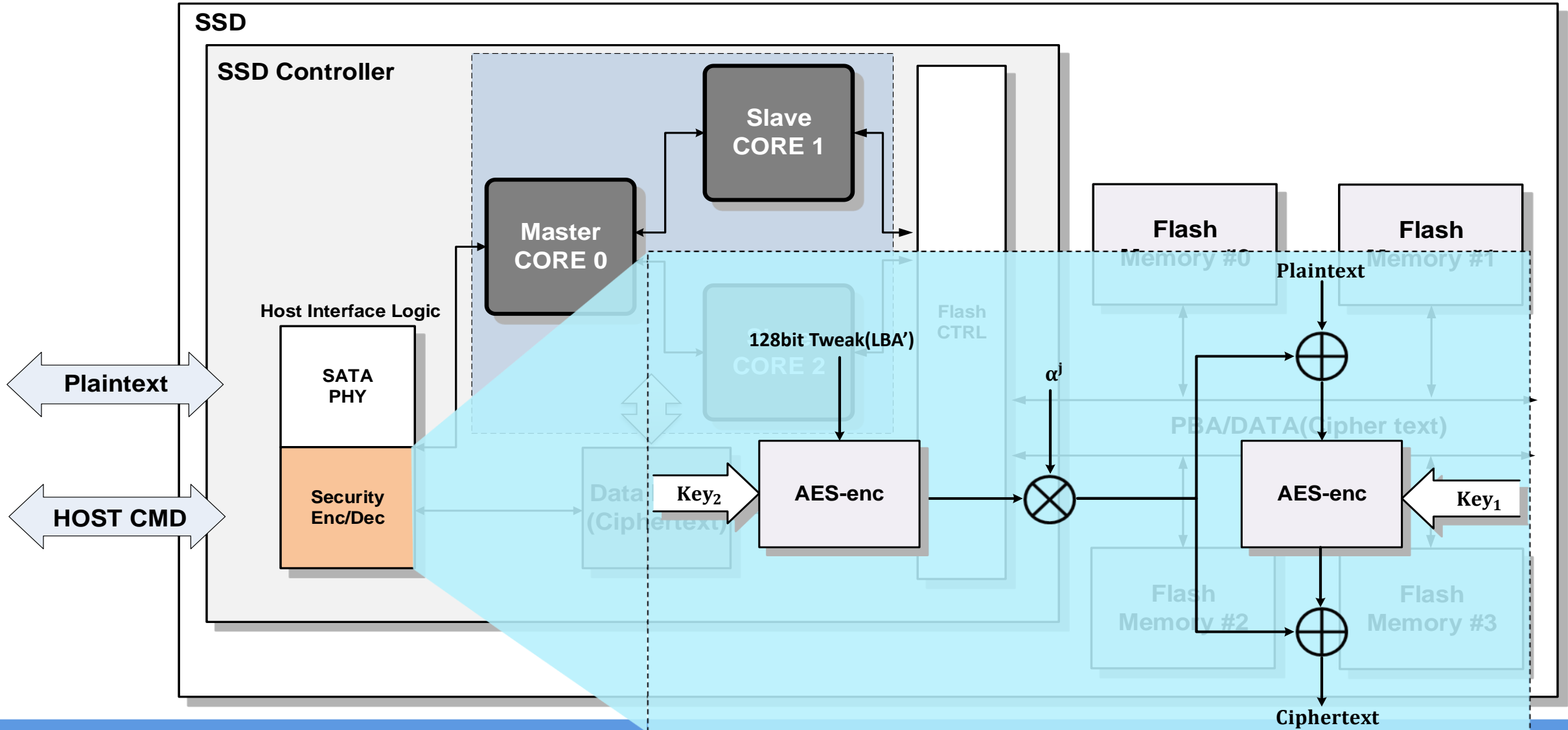
SSD Hardware Architecture

- Multi Core based SSD Controller

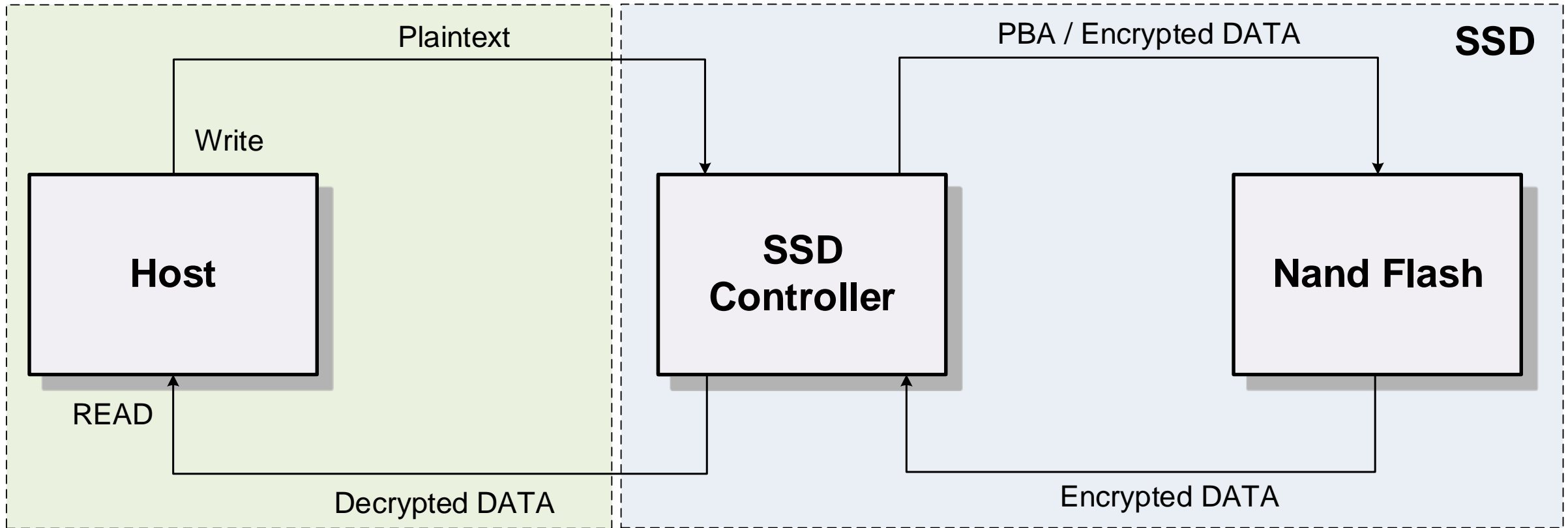


SSD Hardware Architecture

■ AES-XTS



Security Encoding and Decoding



You can Buy Now 2020



Regular shopping cart | Shopping only

shopping basket > Order/Payment > complete

- Cart items are stored for up to 30 days.
- If information such as price or options has changed, you may not be able to order.
- As for today's departure products, today's departure may change depending on the seller's setting point, so please check again when placing an order.



Security Encoding SSD



Product information	option	ATA Interface
 <p>Reproduction System Smart Store N Pay + Samsung SSD 850 PRO 128GB / MZ-7KE128B/KR Bull et Delivery 95,000 KRW 11. 12. (Thu) 90% probability of arrival</p>	Product order quantity: 1 <input type="button" value="Add/Change order conditions"/>	<div style="border: 1px solid black; padding: 5px; text-align: center;">ATA Interface</div> <div style="border: 1px solid black; padding: 5px; text-align: center; background-color: red; color: white; font-weight: bold;">AES Crypto Engine</div> <div style="border: 1px solid black; padding: 5px; text-align: center;">DRAM</div> <div style="border: 1px solid black; padding: 5px; text-align: center;">CPU</div>
 <p>Compuzone Smart Store N Pay + Micron Crucial MX500 Series 250GB TLC KRW 45,550 11. 12. (Thursday) 94% probability of arrival</p>	Product order quantity: 1 <input type="button" value="Add/Change order conditions"/>	<div style="border: 1px solid black; padding: 5px; text-align: center;">Flash Controller</div> <div style="display: flex; justify-content: space-around;"> <div style="border: 1px solid black; padding: 5px; text-align: center;">NAND Flash</div> <div style="border: 1px solid black; padding: 5px; text-align: center;">NAND Flash</div> <div style="border: 1px solid black; padding: 5px; text-align: center;">NAND Flash</div> <div style="border: 1px solid black; padding: 5px; text-align: center;">NAND Flash</div> </div>

Non-Security Encoding SSD



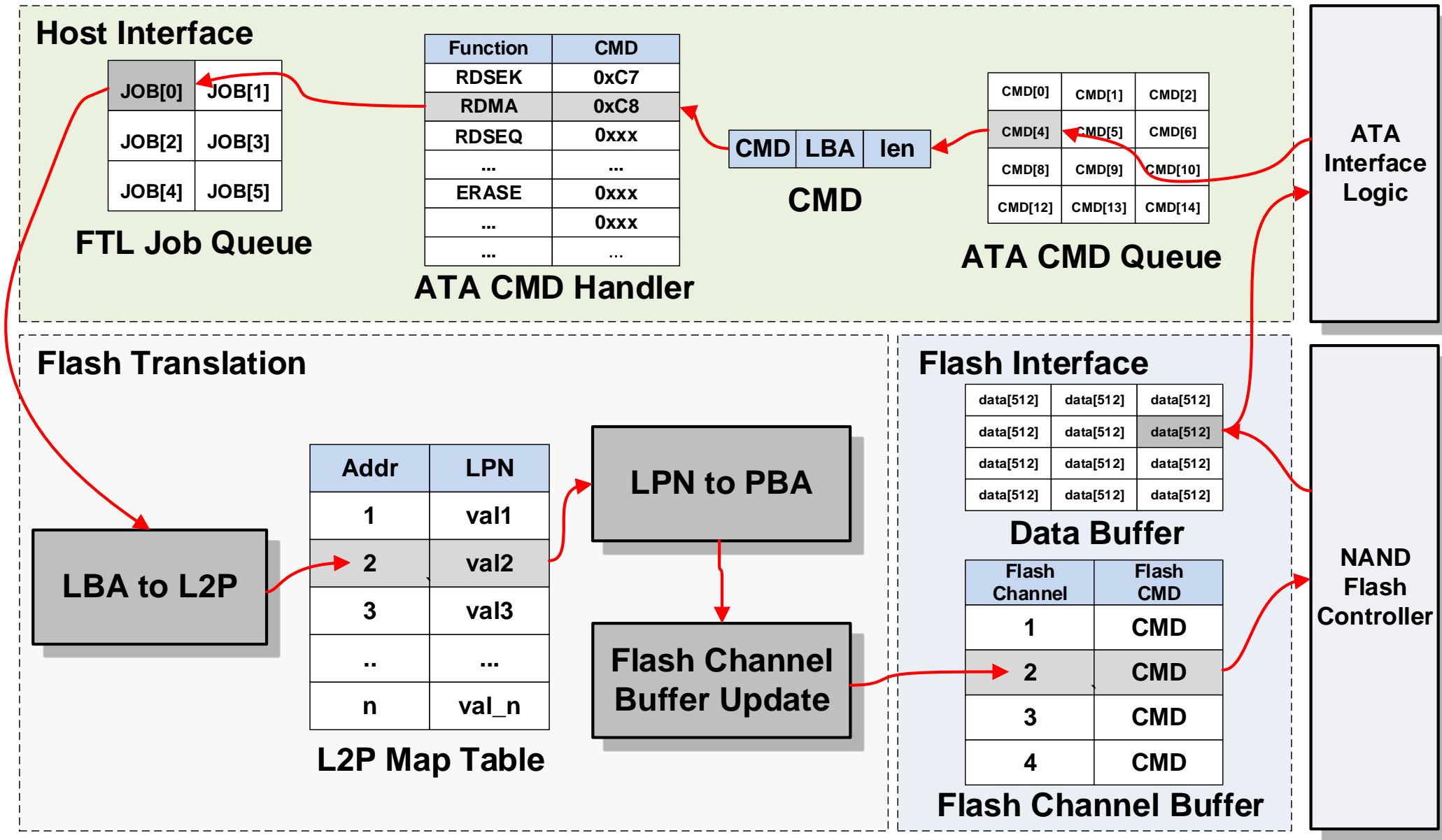
 <p>N Premium Shopping Mall Smart Store N Pay + TeamGroup GX2 (128GB) SSD hard HOT product 22,500 won 11. 11.(Wed) 95% probability of arrival</p>	Product order quantity: 1 <input type="button" value="Add/Change order conditions"/>	<div style="border: 1px solid black; padding: 5px; text-align: center;">ATA Interface</div> <div style="border: 1px dashed black; padding: 5px; text-align: center;">DRAM</div> <div style="border: 1px dashed black; padding: 5px; text-align: center;">CPU</div>
 <p>Myssd Smart Store N Pay + Review Announcement SSD 900G Blue 2.5 inch SATA 240GB Genuine Bulk Packaging Warranty 5 years 32,800 KRW 36,300 11. 12. (Thu) 98% probability of arrival</p>	Product order quantity: 1 <input type="button" value="Add/Change order conditions"/>	<div style="border: 1px solid black; padding: 5px; text-align: center;">Flash Controller</div> <div style="display: flex; justify-content: space-around;"> <div style="border: 1px solid black; padding: 5px; text-align: center;">NAND Flash</div> <div style="border: 1px solid black; padding: 5px; text-align: center;">NAND Flash</div> <div style="border: 1px solid black; padding: 5px; text-align: center;">NAND Flash</div> <div style="border: 1px solid black; padding: 5px; text-align: center;">NAND Flash</div> </div>

quantity

SSD Firmware Reversing

Access All Physical Block

SSD Read Sequence Workflow



ATA CMD Queue

Host Interface Layer

ATA CMD: 0xC8(READ CMD)

Sector Size(8bit) : 0x05

LBA(24bit) : 0xE0A5A5A5

SD:20000000	00000000	00000000	00001459	00008000	NNNNNNNNYcNNNNNN
SD:20000010	00000010	00000000	00000000	00004032	UUUUUUUUU8UUUUUU
SD:20000020	00000000	00000410	00000F3F	00000000	NNNNNNNNNNNN2@UU
SD:20000030	00000001	00000000	00000005	00000000	NNNNNDENN?SNNNNNN
SD:20000040	00008027	000000C8	E0A5A5A9	00000000	UUUUULTUU?IUUUUU
SD:20000050	00000000	00000000	00000000	C708F991	SNNNNNNNNNNNNNN
SD:20000060	124F782F	00002000	E0A5A5A5	00000000	HUUUUUUUUUUUUUU
SD:20000070	00000005	00000000	00000000	00000A00	'NNCNCNNNAAAENNN
SD:20000080	00000000	00006739	00000000	0000011C	UUUBUUU9550UUUU
SD:20000090	00008EE0	00000000	00000009	808B483F	NNNNNNNNNNNN4FBC
SD:200000A0	00000000	04000C00	000000B3	F9BD13F7	NNNNNNNNNNNN1957
SD:200000B0	000513E5	000801E5	00001D81	7FA06000	UUUUUUUUUUUUUUUU
SD:200000C0	00000008	00004BFF	00000000	00000000	ENNNNNNNNNNNLNN
SD:200000D0	00010001	30002BF2	00260200	8050280D	UUUUUUUUUUUUUFUU
SD:200000E0	0075320D	0D054141	B24B1030	0E390157	NNNN9gNNNNNNFSNN
SD:200000F0	00000014	00000000	00000000	00000000	UUUUUUUUUUUUUSHUU
SD:20000100	00000000	00000000	00000000	00000000	ENNNNNNNNNNN?HBB
SD:20000110	00820005	00000000	00000000	00000000	UUUUUUUUUUUUUBO
SD:20000120	3F027731	0E8E0001	03AE6260	40800C00	NNNNNNNNNNNNFCBF
SD:20000130	80730001	00000000	E0A5A5A5	00000000	UUUUUUUUUUUUUD9
SD:20000140	00000000	00000000	00000000	00000000	EGENESBNN&CNNN'A/
SD:20000150	9F000000	00000000	00000000	00000000	UUUUUUUUUUUUUF
SD:20000160	040113E5	00820000	00000000	00000000	VNNNFkNNNNNNNNNN
SD:20000170	00000000	00000000	00000000	00000000	TUUUFkUUUUUUUUUU
SD:20000180	00000000	000A000A	0000A5A5	00000000	SNSNE+UNOVS&NC(PB
SD:20000190	03020100	07060504	00000000	00000000	HUUHU2+UUUXUR(PB
SD:200001A0	E0A5A5A5	C8000000	00000005	80A5A5A5	C2uNAAECORLKBW9S
SD:200001B0	00040000	00000000	00000000	00000000	UUUUUUUUUUUUUUUU

ATA CMD Handler

Host Interface Layer

```

ROM:0000C50C
ROM:0000C50C
ROM:0000C50C
ROM:0000C50C      sub_C50C
ROM:0000C50C F0 5F 2D E9 PUSH      {R4-R12,LR}
ROM:0000C510 03 10 D0 E5 LDRB      R1, [R0,#3]
ROM:0000C514 8C 21 9F E5 LDR      R2, =sata_handler_table
ROM:0000C518 7C 41 9F E5 LDR      R4, =000F0_1A298
ROM:0000C51C 81 11 61 E0 RSB      R1, R1, R1,LSL#3
ROM:0000C520 02 50 81 E0 ADD      R5, R1, R2
ROM:0000C524 01 10 95 E5 LDR      R1, [R5,#1]
ROM:0000C528 D4 61 C4 E1 LDRD      R6, R7, [R4,#0x14]
ROM:0000C52C 00 00 51 E3 CMP      R1, #0
ROM:0000C530 54 00 00 0A BEQ      loc_C688
    
```

```

ROM:0000C5C0
ROM:0000C5C0      loc_C5C0
ROM:0000C5C0 01 20 95 E5 LDR      R2, [R5,#1]
ROM:0000C5C4 B5 10 D5 E1 LDRH      R1, [R5,#5]
ROM:0000C5C8 32 FF 2F E1 BLX      R2
ROM:0000C5CC 00 00 50 E3 CMP      R0, #0
ROM:0000C5D0 01 00 A0 03 MOVEQ     R0, #1
ROM:0000C5D4 04 00 C4 05 STRBEQ   R0, [R4,#(byte_1A29C - 0x1A298)]
ROM:0000C5D8 B5 00 D5 E1 LDRH      R0, [R5,#5]
ROM:0000C5DC 01 0C 10 E3 TST      R0, #0x100
ROM:0000C5E0 14 00 00 0A BEQ      loc_C638
    
```

ATA CMD Handler Table

seg002:00808B42	00	DCB	0
seg002:00808B43	00	DCB	0
seg002:00808B44	C4	DCB	0xC4
seg002:00808B45	65 0B 01 00	DCD	sub_10B64+1
seg002:00808B49	07	DCB	7
seg002:00808B4A	01	DCB	1
seg002:00808B4B	C5	DCB	0xC5
seg002:00808B4C	78 F5 00 00	DCD	sub_F578
seg002:00808B50	06	DCB	6
seg002:00808B51	01	DCB	1
seg002:00808B52	C6	DCB	0xC6
seg002:00808B53	D7 08 00 80	DCD	sub_800008D6+1
seg002:00808B57	00	DCB	0
seg002:00808B58	00	DCB	0
seg002:00808B59	00	DCB	0
seg002:00808B5A	BD CC 00 00	DCD	sub_CCBC+1
seg002:00808B5E	00	DCB	0
seg002:00808B5F	00	DCB	0
seg002:00808B60	C8	DCB	0xC8
seg002:00808B61	AC 03 01 00	DCD	RDMA Handler
seg002:00808B65	01	DCB	1
seg002:00808B66	01	DCB	1
seg002:00808B67	C9	DCB	0xC9
seg002:00808B68	AC 03 01 00	DCD	RDMA Handler
seg002:00808B6C	01	DCB	1
seg002:00808B6D	01	DCB	1
seg002:00808B6E	CA	DCB	0xCA
seg002:00808B6F	78 F5 00 00	DCD	sub_F578

 : ATA Command : Handler Function

Flash Chip → Flash DATA Buffer []

- Flash Interface Layer → Flash Chip → Flash Interface Layer

code: str r1, [r0]
r1: '0x00'
r0: Flash Channel Buffer Address

Flash Interface Layer

Channel	CMD
0	CMD2
1	CMD1
2	CMD3
3	CMD0

Flash Channel Buffer

Encrypted Data

Flash Data Buffer

Flash Data Buffer [] → Host Interface Logic

- Flash Interface Layer → Host Interface Layer → Host PC

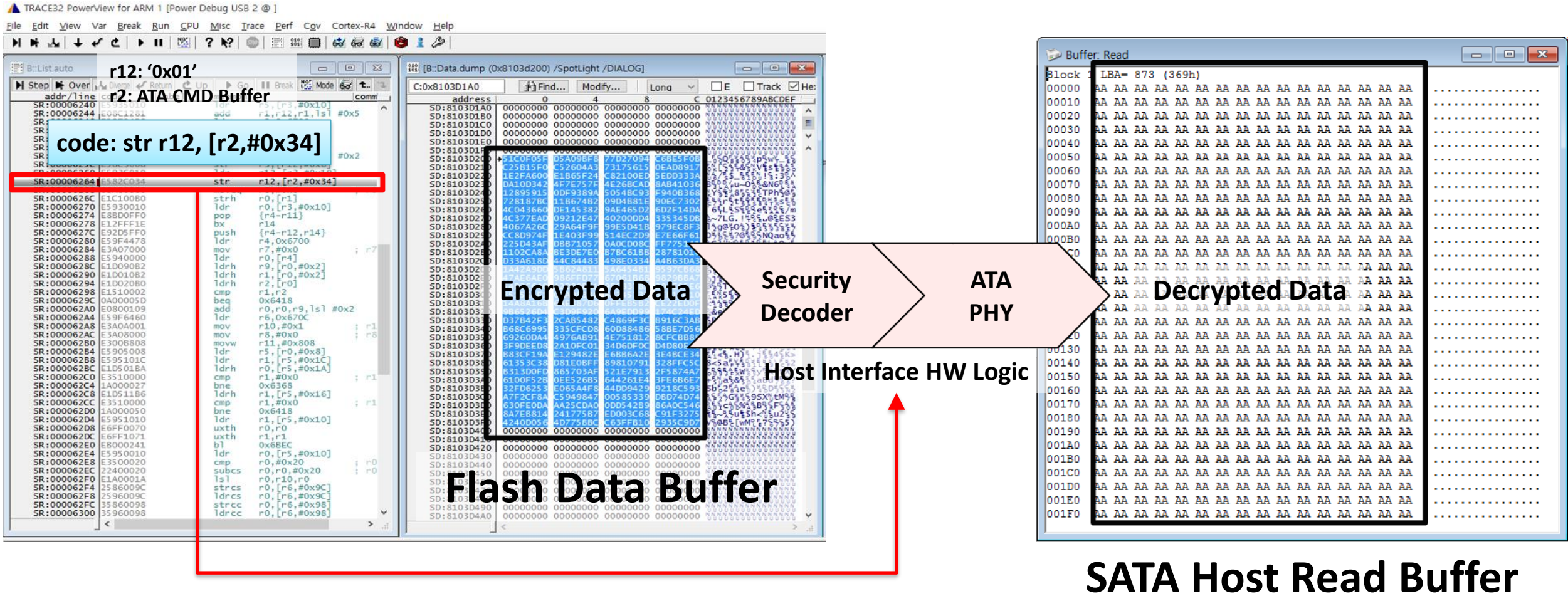
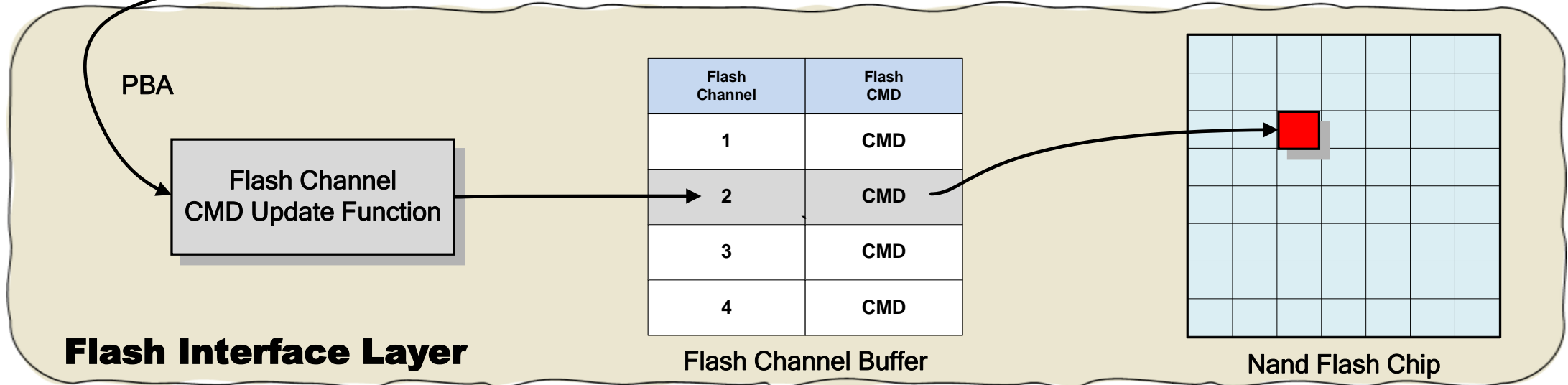
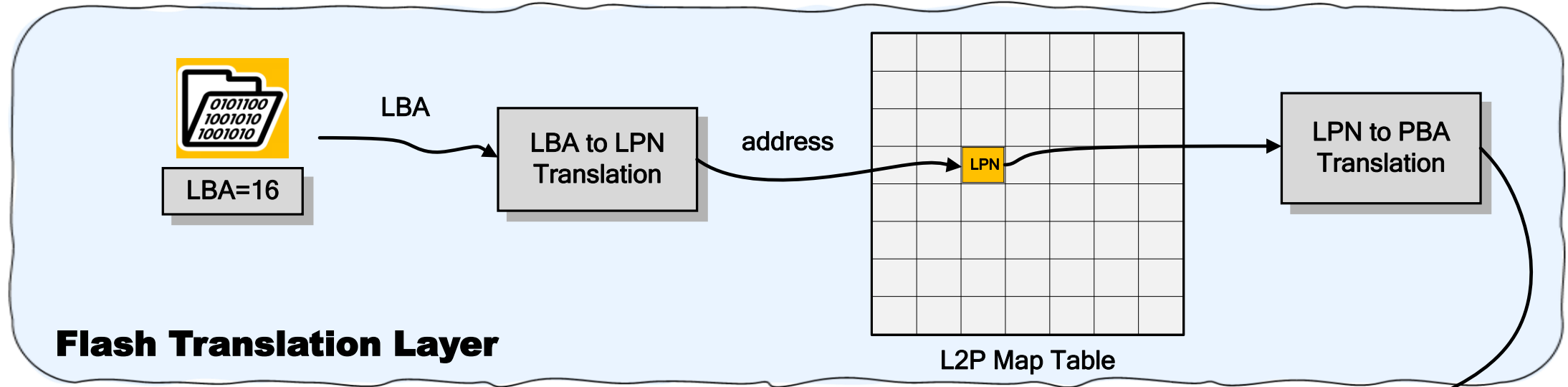


Figure Out Where PBA and Channel Buffer are



L2P Map Table

Flash Translation Layer

The image shows two memory dump windows for Core 1 and Core 2. Each window displays a list of memory addresses and their corresponding data. Four channels are highlighted in yellow boxes at the bottom of each window:

- Channel 0: 853CB600 (Core 1), 8B7CB600 (Core 2)
- Channel 1: 8618E400 (Core 1), 8C58E400 (Core 2)
- Channel 2: 86EBAE00 (Core 1), 8D2BAE00 (Core 2)
- Channel 3: 87BE7800 (Core 1), 8DFE7800 (Core 2)

Arrows point from these channel labels to the corresponding memory addresses in the dump windows.

The image shows a memory dump window titled "[B::d.dump 0x8b8a0000 /SpotLight]". The window displays a list of memory addresses and their corresponding data. A blue box labeled "Using Area" highlights a region of memory starting at address 8B88C7B0. A green box labeled "Empty AREA" highlights a region of memory starting at address 8B88C920.

address	0	4	8	C	0123456789ABCDEF
SD:8B88C760	03B63303	3203CB3E	CB3F03CB	03CB3303	E3E3E3>CE2CE?CE3CE
SD:8B88C770	3423603E	603F0394	03943523	34238D3E	>`#4#4?`#5#4>#4
SD:8B88C780	8D3F0355	03553523	3423863E	863F03B6	U#?#5U#>#4#?#
SD:8B88C790	03B63523	3423CB3E	CB3F03CB	03CB3523	#5#>#4#?#5#
SD:8B88C7A0	36039440	94410394	03943703	36035540	@#6#4#>#4#?#6
SD:8B88C7B0	55410355	03553703	3603B640	B64103B6	@#6#4#>#4#?#6
SD:8B88C7C0	03B63703	3203CB3E	CB3F03CB	03CB3703	#7#>#4#?#5#
SD:8B88C7D0	38236042	603F0394	03943523	38238D40	@`#8#4#A`#9#4#>#8
SD:8B88C7E0	8D410355	03553703	3603B640	B64103B6	U#A#9U#>#8#A#
SD:8B88C7F0	03B63923	3823CB40	CB4103CB	03CB3923	#9#>#4#?#5#
SD:8B88C800	3A039442	94430394	03943B03	3A035542	B#>#4#?#5#
SD:8B88C810	55430355	03553B03	3C03B642	8D430355	U#CU#;U#B#<U#C#
SD:8B88C820	03553D23	3A238642	B64303B6	03B63B03	#=U#B#;#5#C#>#4#
SD:8B88C830	3A03CB42	CB4303CB	03CB3B03	3C236042	B#>#4#?#5#
SD:8B88C840	60430394	03943D23	FF238D42	FFFFFFFF	#>#4#?#5#
SD:8B88C850	FFFFFFFF	FFFFFFFF	FFFFFFFF	FFFFFFFF	FFFFFFFFFFFFFFFFFFFF
SD:8B88C860	FFFFFFFF	FFFFFFFF	FFFFFFFF	FFFFFFFF	FFFFFFFFFFFFFFFFFFFF
SD:8B88C870	FFFFFFFF	FFFFFFFF	FFFFFFFF	FFFFFFFF	FFFFFFFFFFFFFFFFFFFF
SD:8B88C880	FFFFFFFF	FFFFFFFF	FFFFFFFF	FFFFFFFF	FFFFFFFFFFFFFFFFFFFF
SD:8B88C890	FFFFFFFF	FFFFFFFF	FFFFFFFF	FFFFFFFF	FFFFFFFFFFFFFFFFFFFF
SD:8B88C8A0	FFFFFFFF	FFFFFFFF	FFFFFFFF	FFFFFFFF	FFFFFFFFFFFFFFFFFFFF
SD:8B88C8B0	FFFFFFFF	FFFFFFFF	FFFFFFFF	FFFFFFFF	FFFFFFFFFFFFFFFFFFFF
SD:8B88C8C0	FFFFFFFF	FFFFFFFF	FFFFFFFF	FFFFFFFF	FFFFFFFFFFFFFFFFFFFF
SD:8B88C8D0	FFFFFFFF	FFFFFFFF	FFFFFFFF	FFFFFFFF	FFFFFFFFFFFFFFFFFFFF
SD:8B88C8E0	FFFFFFFF	FFFFFFFF	FFFFFFFF	FFFFFFFF	FFFFFFFFFFFFFFFFFFFF
SD:8B88C8F0	FFFFFFFF	FFFFFFFF	FFFFFFFF	FFFFFFFF	FFFFFFFFFFFFFFFFFFFF
SD:8B88C900	FFFFFFFF	FFFFFFFF	FFFFFFFF	FFFFFFFF	FFFFFFFFFFFFFFFFFFFF
SD:8B88C910	FFFFFFFF	FFFFFFFF	FFFFFFFF	FFFFFFFF	FFFFFFFFFFFFFFFFFFFF
SD:8B88C920	FFFFFFFF	FFFFFFFF	FFFFFFFF	FFFFFFFF	FFFFFFFFFFFFFFFFFFFF
SD:8B88C930	FFFFFFFF	FFFFFFFF	FFFFFFFF	FFFFFFFF	FFFFFFFFFFFFFFFFFFFF

LPN → PBA Translation

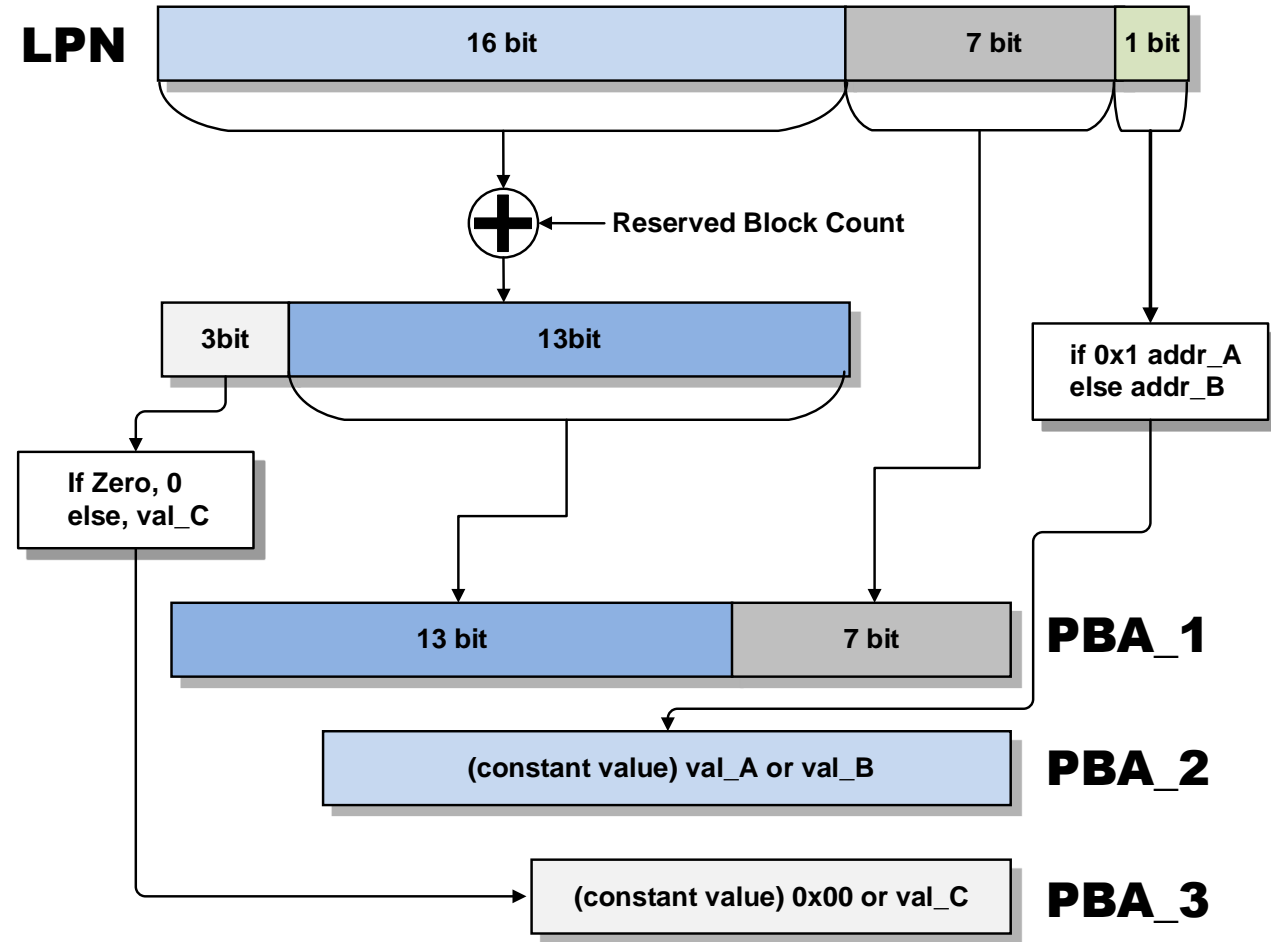
Flash Translation Layer

```
ROM:000077D8
ROM:000077D8
ROM:000077D8
ROM:000077D8 PBA_calcl
ROM:000077D8 78 85 PUSH {R4,R6,LR}
ROM:000077DA 06 46 MOV R6, R0
ROM:000077DC 40 F2 A8 78 MOVW R0, #0x7AB

ROM:000286C CB 4B LDR R3, =channel_count
ROM:000286E CE 4D LDR R5, =dword_1C7E8
ROM:0002870 11 6A LDR R1, [R2,#0x20]
ROM:0002872 9C 6C LDR R4, [R3,#(dword_1C718 - 0x1C6D0)]
ROM:0002874 D5 F8 E0 51 LDR.W R5, [R5,#(dword_1C9C8 - 0x1C7E8)]
ROM:0002878 DF 6C LDR R7, [R3,#(dword_1C71C - 0x1C6D0)]
ROM:000287A 21 FA 04 F4 LSR.W R4, R1, R4
ROM:000287E 66 19 ADDS R6, R4, R5
ROM:0002880 D3 F8 B4 50 LDR.W R5, [R3,#(dword_1C784 - 0x1C6D0)]
ROM:0002884 5B 6C LDR R3, [R3,#(dword_1C714 - 0x1C6D0)]
ROM:0002886 26 FA 05 F4 LSR.W R4, R6, R5
ROM:000288A AF 40 LSL.S R7, R5
ROM:000288C 7F 1E SUBS R7, R7, #1
ROM:000288E 5B 1E SUBS R3, R3, #1

ROM:00014858
ROM:00014858
ROM:00014858
ROM:00014858
ROM:00014858 sub_14858
ROM:00014858 02 46 MOV R2, R0
ROM:0001485A 00 20 MOVS R0, #0
ROM:0001485C 62 F3 DF 10 BFI.W R0, R2, #7, #0x19
ROM:00014860 61 F3 06 00 BFI.W R0, R1, #0, #7
ROM:00014864 70 47 BX LR
ROM:00014864 ; End of function sub_14858
ROM:00014864
```

Raw Code



Logical Expression

LPN → PBA Translation

PBA_1 = ?

13 bit

7 bit

PBA_2 = ?

(constant value) addr_A or addr_B

PBA_3 = ?

(constant value) 0x00 or val_C



Plane

Block

Page

Page

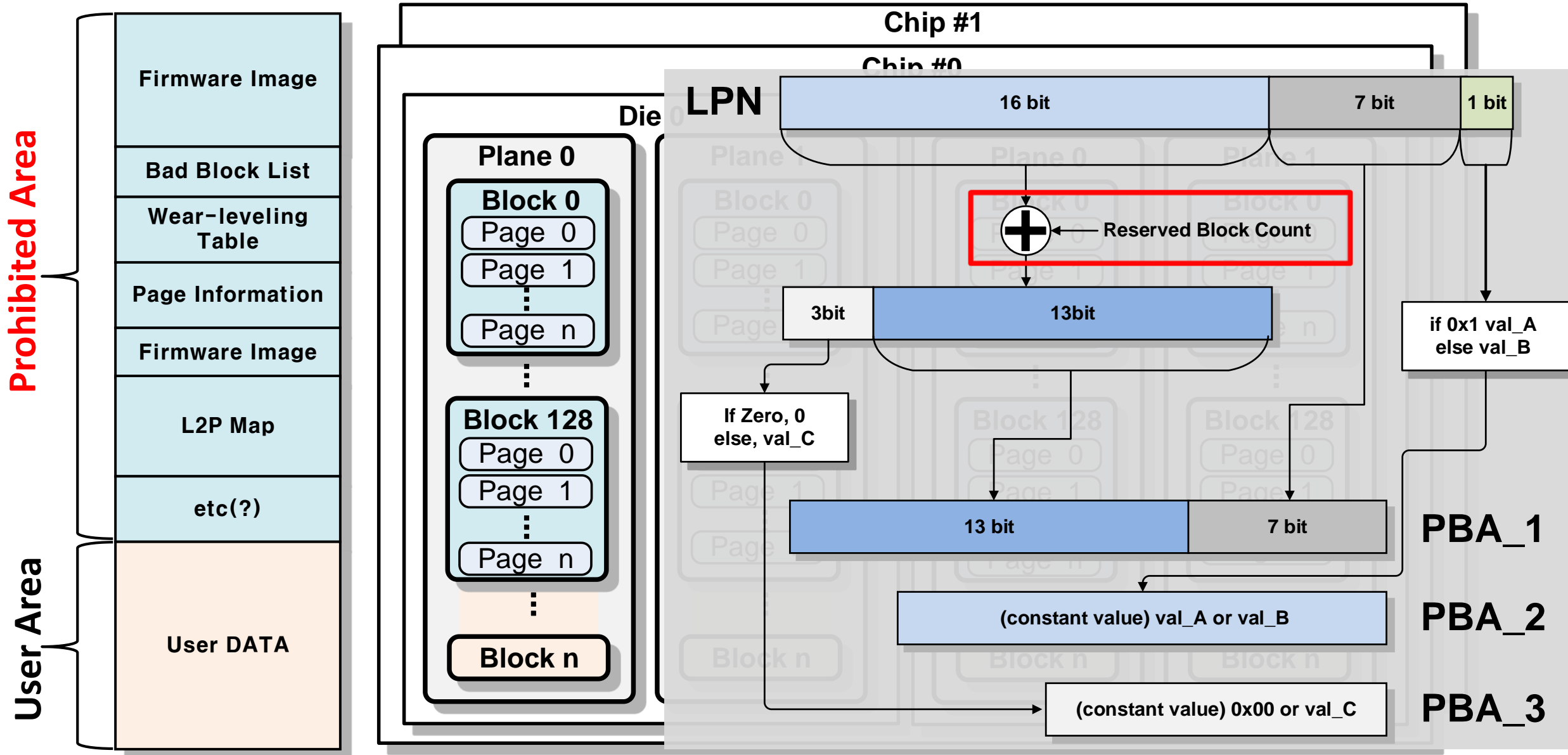
Page

Way

Flash

CH

LPN → PBA Translation (Reserved Block Count)



Flash Channel Buffer

Flash Interface Layer

The screenshot displays the TRACE32 PowerView interface for ARM 3, showing four data dump windows for different channels. The windows are labeled Channel 0 (red), Channel 1 (blue), Channel 2 (green), and Channel 3 (yellow). Each window shows a list of data points with columns for address, data, and other parameters. Two callouts highlight specific data points:

- NAND Flash CMD (Parameter):** Located in the Channel 2 window, highlighting a data point with address 0x204A0003 and value 00000701.
- NAND Flash CMD (Primary):** Located in the Channel 2 window, highlighting a data point with address 0x204E01E0 and value 00000000.

The interface also shows a list of variables on the left and a status bar at the bottom indicating the current state of the system.

NAND Flash Command in Flash Channel Buffer

Flash Interface Layer

010
101 B::d.dump 0x204d0240

address	0	4	8	C	0123456789ABCDEF
SD:204D0240	00000007	00000001	00000000	00000000	NNNNNNNNNNNNNNNN
SD:204D0250	00000000	00000000	00000000	00000000	UUUUUUUUUUUUUUUU
SD:204D0260	00000000	00000000	00000000	00000000	NNNNNNNNNNNNNNNN
SD:204D0270	00000000	00000000	00000000	00000000	UUUUUUUUUUUUUUUU
SD:204D0280	00000000	00000000	00000000	00000000	NNNNNNNNNNNNNNNN
SD:204D0290	00000000	00000000	00000000	00000000	UUUUUUUUUUUUUUUU
SD:204D02A0	00000000	00000000	00000000	00000000	NNNNNNNNNNNNNNNN
SD:204D02B0	00000000	00000000	00000000	00000000	UUUUUUUUUUUUUUUU
SD:204D02C0	00000000	00000000	00000000	00000000	NNNNNNNNNNNNNNNN
SD:204D02D0	00000000	00000000	00000000	00000000	UUUUUUUUUUUUUUUU
SD:204D02E0	00000000	00000000	00000000	00000000	NNNNNNNNNNNNNNNN
SD:204D02F0	00000000	00000000	00000000	00000000	UUUUUUUUUUUUUUUU
SD:204D0300	00000000	00000000	00000000	00000000	NNNNNNNNNNNNNNNN
SD:204D0310	00000000	00000000	00000000	00000000	UUUUUUUUUUUUUUUU
SD:204D0320	00000000	00000000	00000000	00000000	NNNNNNNNNNNNNNNN
SD:204D0330	000000CE	000000FF	01200800	00400200	CNNNFNNNNB_SNS@N
SD:204D0340	0A5888B2	00000000	00000000	00003366	EXLNNNNNNNNNF3NN
SD:204D0350	00010002	4154454D	00000028	00000000	SNS@META(UUUUUUUU
SD:204D0360	00000000	00000000	00003366	00000343	NNNNNNNNNF3NNCEN
SD:204D0370	00000000	00000000	00000000	00000000	UUUUUUUUUUUUUUUU
SD:204D0380	00000000	00000000	00000000	00000000	NNNNNNNNNNNNNNNN
SD:204D0390	00000000	00000000	00000000	00000000	UUUUUUUUUUUUUUUU
SD:204D03A0	00000000	00000000	00000000	00000000	NNNNNNNNNNNNNNNN
SD:204D03B0	00000000	00000000	00000000	00000000	UUUUUUUUUUUUUUUU
SD:204D03C0	00000000	00000000	00000000	00000000	NNNNNNNNNNNNNNNN
SD:204D03D0	00000000	00000000	00000000	00000000	UUUUUUUUUUUUUUUU
SD:204D03E0	00000000	00000000	00000000	00000000	NNNNNNNNNNNNNNNN
SD:204D03F0	00000000	00000000	00000000	00000000	UUUUUUUUUUUUUUUU
SD:204D0400	00000000	00000000	00000000	00000000	NNNNNNNNNNNNNNNN
SD:204D0410	00006401	000000FF	80933000	00000000	SNNNFNNNNH8NNNN
SD:204D0420	00000000	01000000	00000000	0000179C	UUUUUUUUUUUUUUUU
SD:204D0430	0000FFFF	83F5D000	00000000	00000000	FFNNNF3NNNNNNNN
SD:204D0440	00000000	00000000	00000000	00000000	UUUUUUUUUUUUUUUU
SD:204D0450	00000000	00000000	00000000	00000000	NNNNNNNNNNNNNNNN
SD:204D0460	00000000	00000000	00000000	00000000	UUUUUUUUUUUUUUUU
SD:204D0470	00000000	00000000	00000000	00000000	NNNNNNNNNNNNNNNN

NAND CMD Identifier (points to 00000007)

READ: 0x1 (points to 00000001)

PBA_3 (points to 00000000)

PBA_1 (points to 00000000)

Readbuffer Block Bitmask (points to 000000FF)

Data Buffer Address (points to 80933000)

NAND Flash CMD (Parameter) (points to the entire row SD:204D0410)

010
101 B::d.dump 0x204a0000

address	0	4	8	C	0123456789ABCDEF
SD:204A0000	00000032	00000701	00000200	FF F0000	2NNNSBNN NNNNFF
SD:204A0010	00000000	00000000	00000000	2280280A	NNNNNNNNNNNNL78"
SD:204A0020	00070001	00000000	00000000	00000000	SNBNNNNNNNNNNNN
SD:204A0030	00070001	00000211	00000000	00000000	SNNNSNNNNNNNNNN
SD:204A0040	00070001	00000022	00000000	00000000	SNNN"NNNNNNNNNN
SD:204A0050	00060001	00000000	00000000	00000000	HULU UUUUUUUUUUU
SD:204A0060	000B0000	00000444	00000000	00000000	SNNN"NNNNNNNNNN
SD:204A0070	000B0000	00000555	00000000	00000000	UUUUUUUUUUUUUUUU
SD:204A0080	000B0000	00000666	00000000	00000000	SNNN"NNNNNNNNNN
SD:204A0090	000B0000	00000777	00000000	00000000	HUKUUUUUUUUUUUU
SD:204A00A0	00000000	00000000	00000000	00000000	NNVN DENNNNNNNNN
SD:204A00B0	00000000	00000000	00000000	00000000	UUUUUUUUUUUUUUUU
SD:204A00C0	00000000	00000000	00000000	00000000	NNNN"NNNNNNNNNN
SD:204A00D0	00000000	00000000	00000000	00000000	UUUUUUUUUUUUUUUU
SD:204A00E0	00000000	00000000	00000000	00000000	NNNN"NNNNNNNNNN

Offset (points to 00000032)

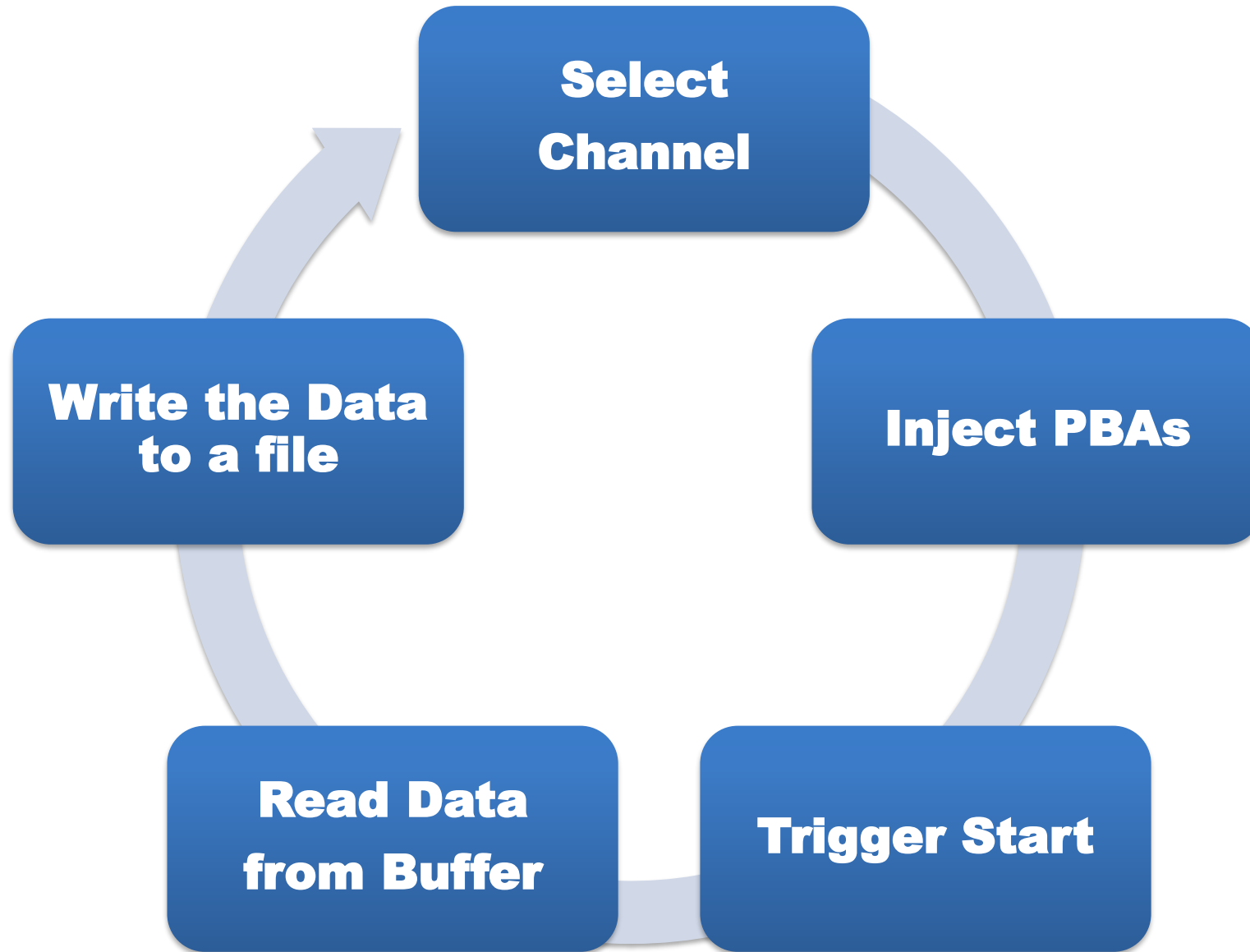
NAND CMD Start Trigger (points to 00000701)

PBA_2 (points to 00000200)

R/W (points to FF F0000)

NAND Flash CMD (Primary) (points to the entire row SD:204A0000)

Steps : Access All Physical Block



DEMO : Access All Physical Block



Okay, then what can we do with it?

- **Non Security Encoding-SSD**
 - **Data Restoration**
 - ✓ **Unique PBA blocks not found in the LBA**
 - **Forensics**
 - ✓ **Image based on LBA → Image based on PBA**
 - ✓ **Non-Destructive**

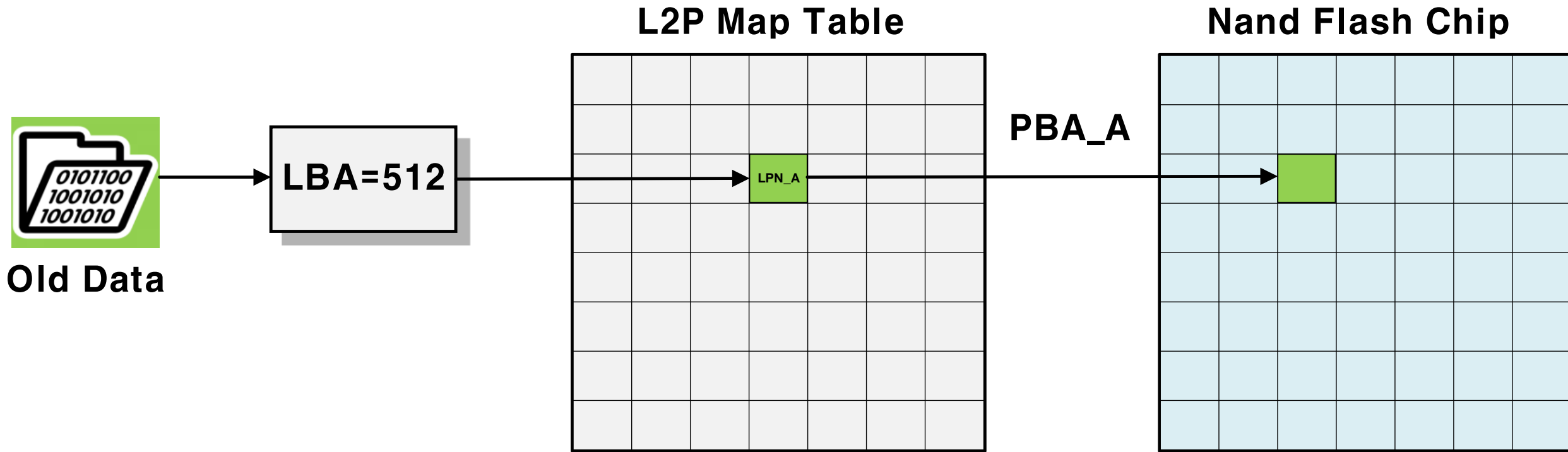
Okay, then what can we do with it?

- **Security Encoding-SSD**
 - **Secure Erase Verification**
 - ✓ **Whether SSD still leaves sensitive data or not**
 - **Access to Factory Reserved Area**
 - ✓ **You may find Critical Information in SSD**
 - ✓ **Generally, Not Encrypted**

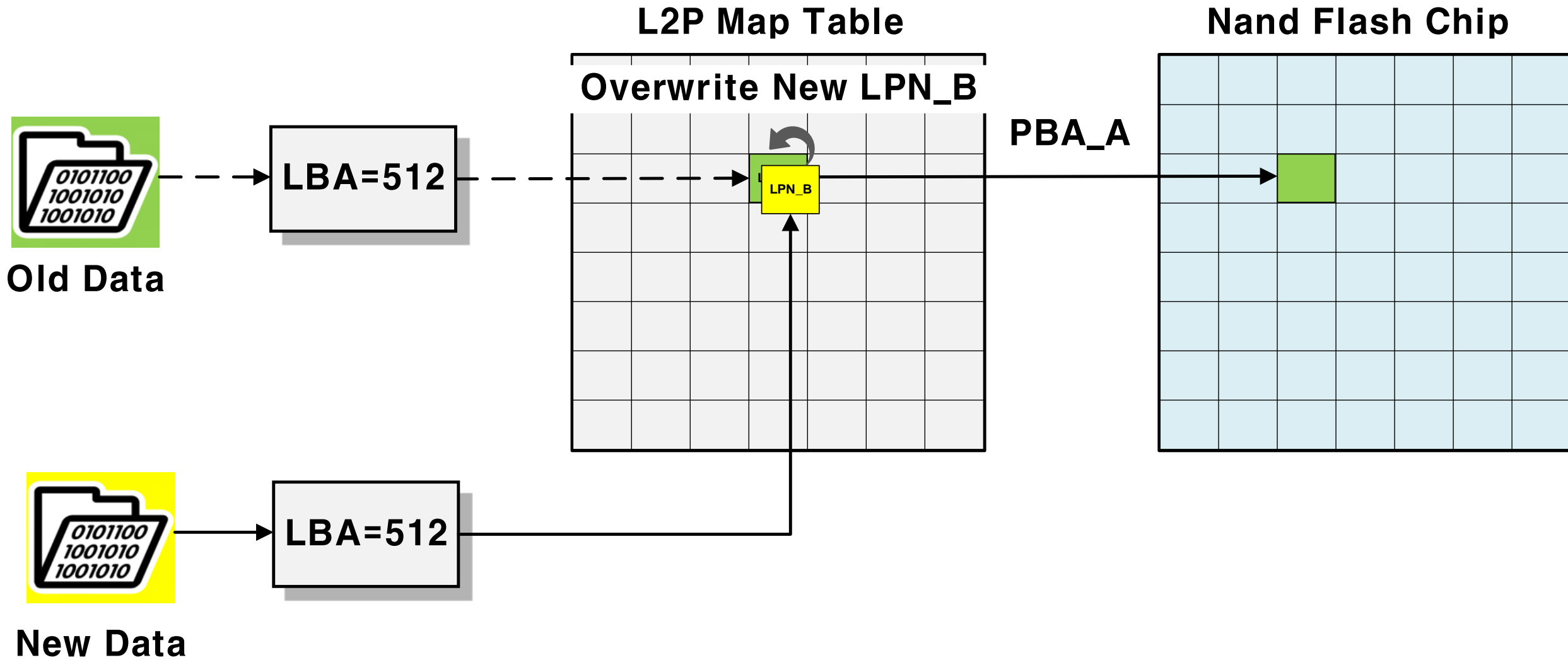
SSD Firmware Reversing

Recover Overwritten Data

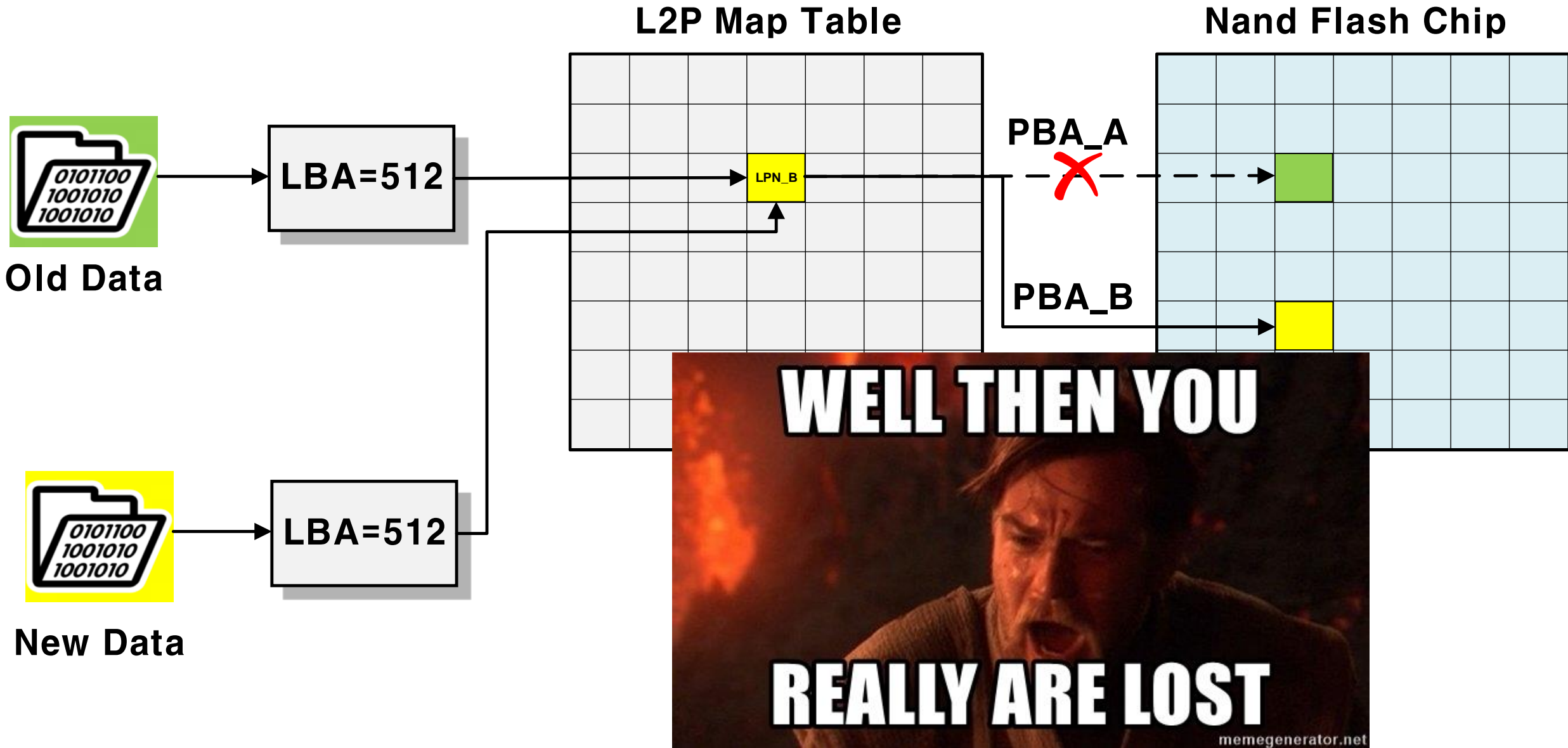
Overwrite to Same LBA



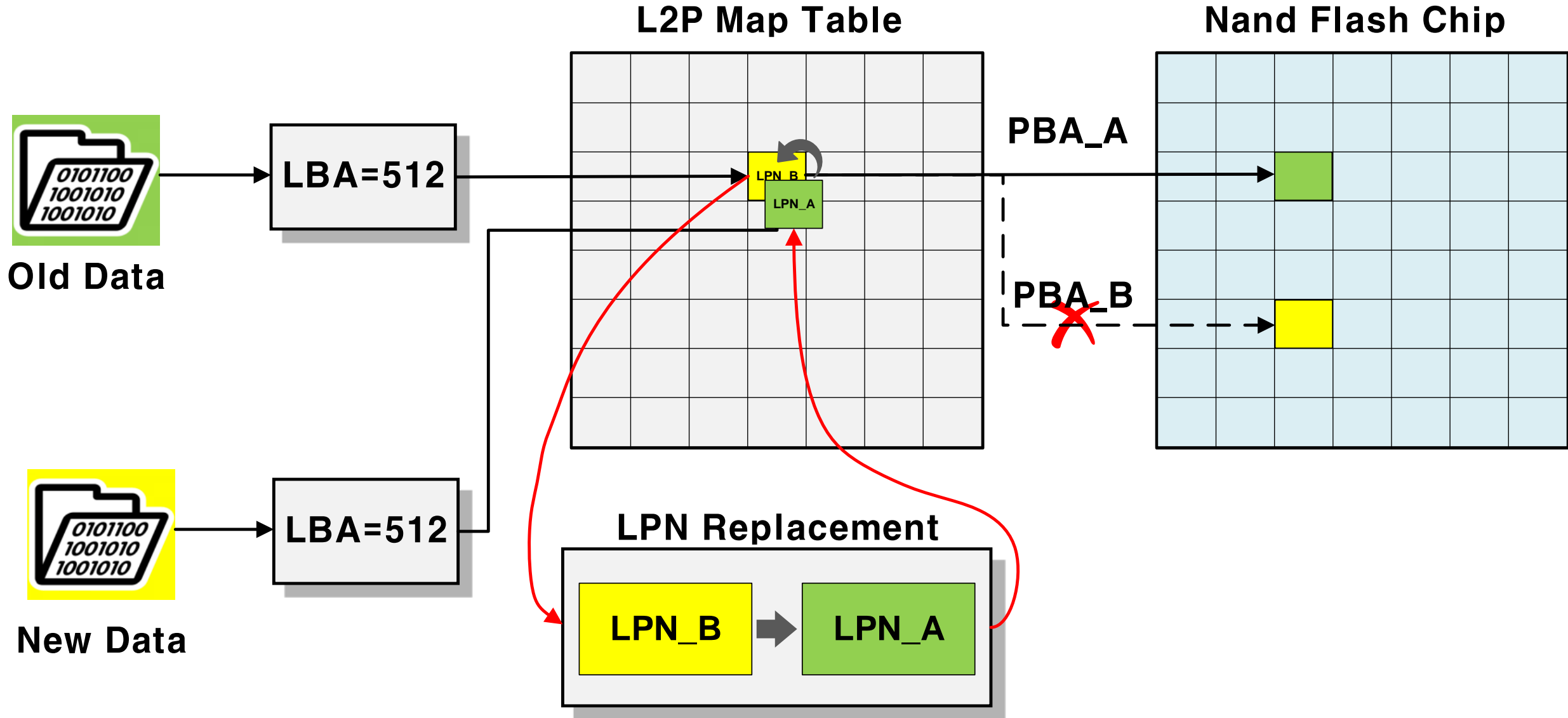
Overwrite to Same LBA



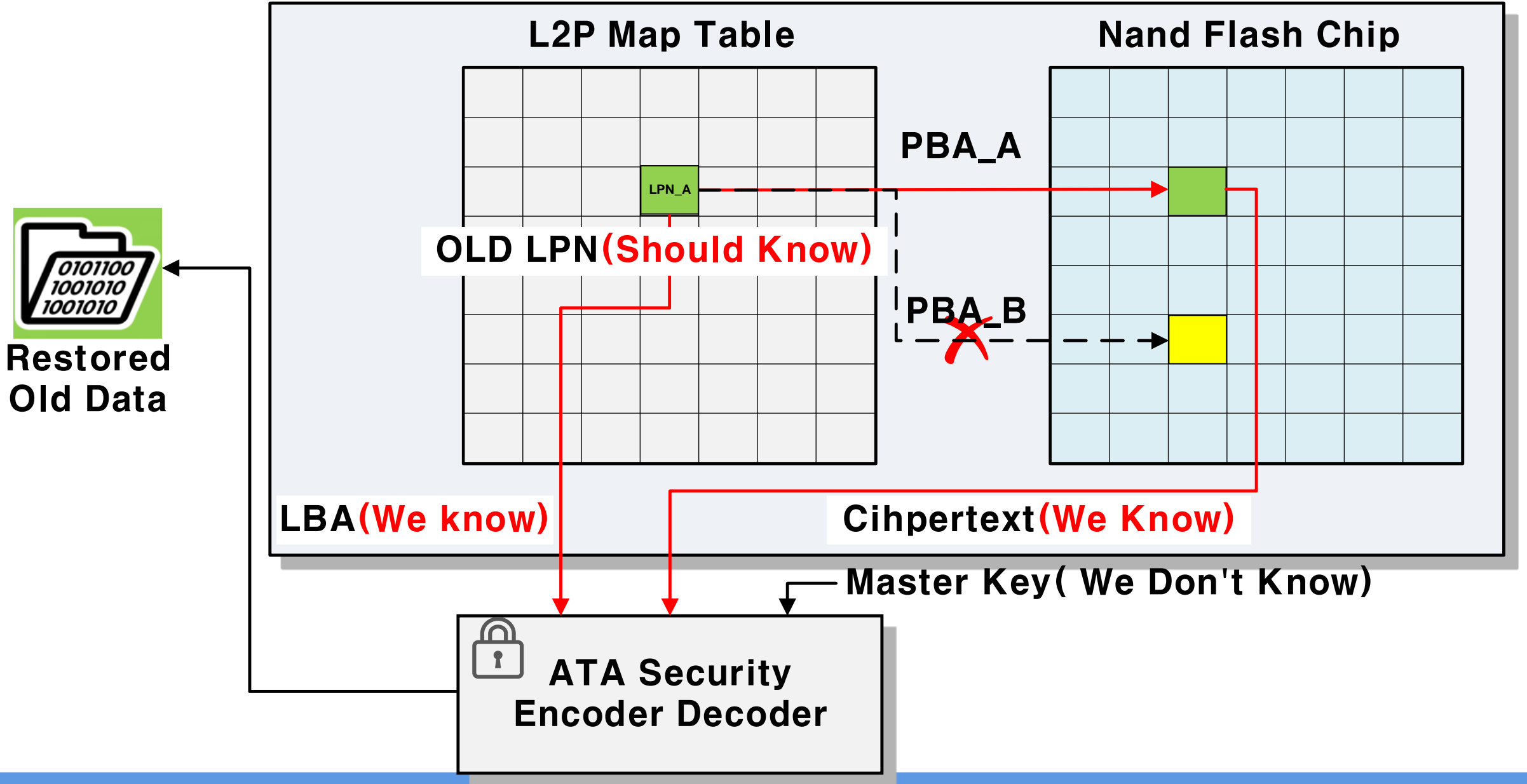
Overwrite to Same LBA



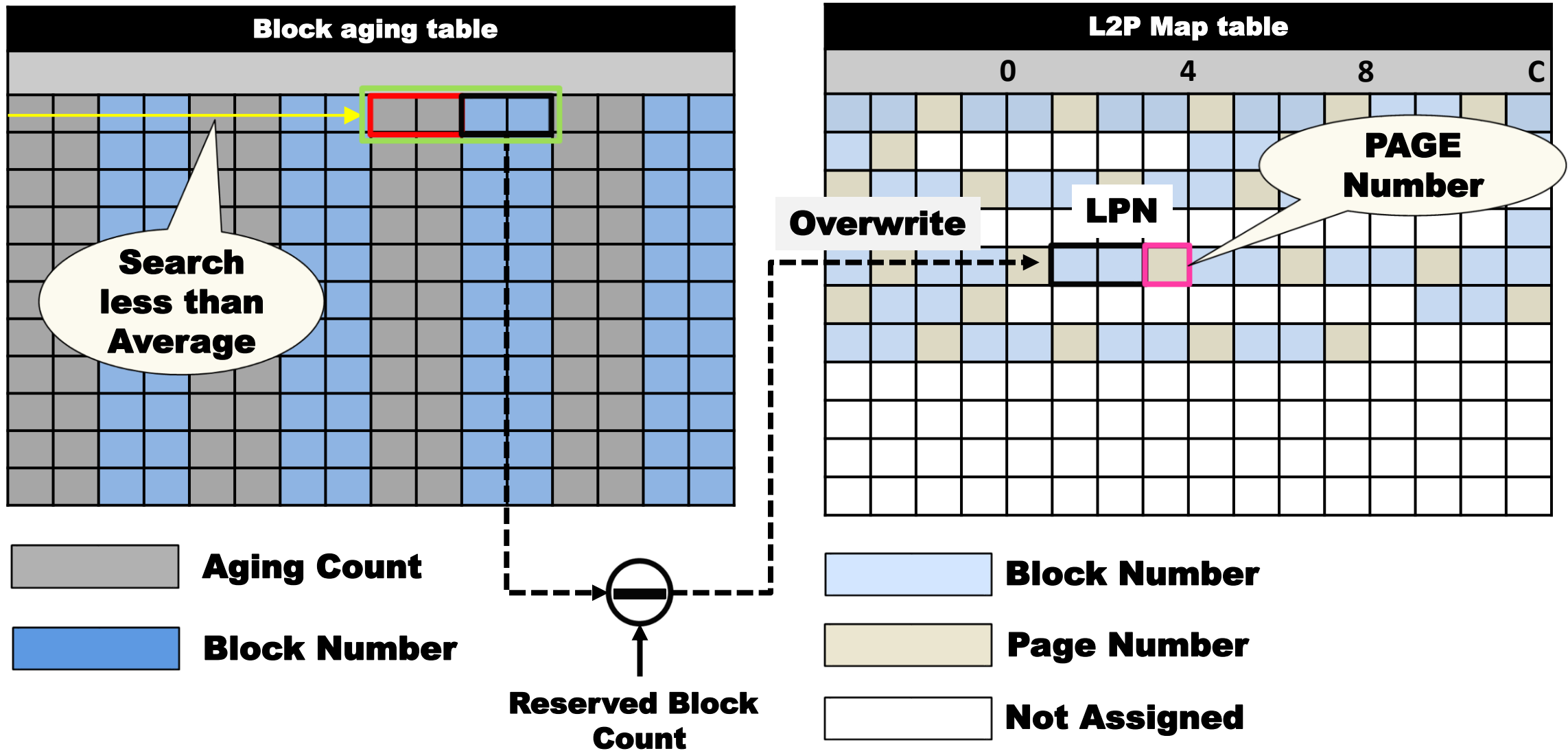
IS It Still Alive?



Now, What we Know & Don't know & Should know



Block aging table and Data Overwriting

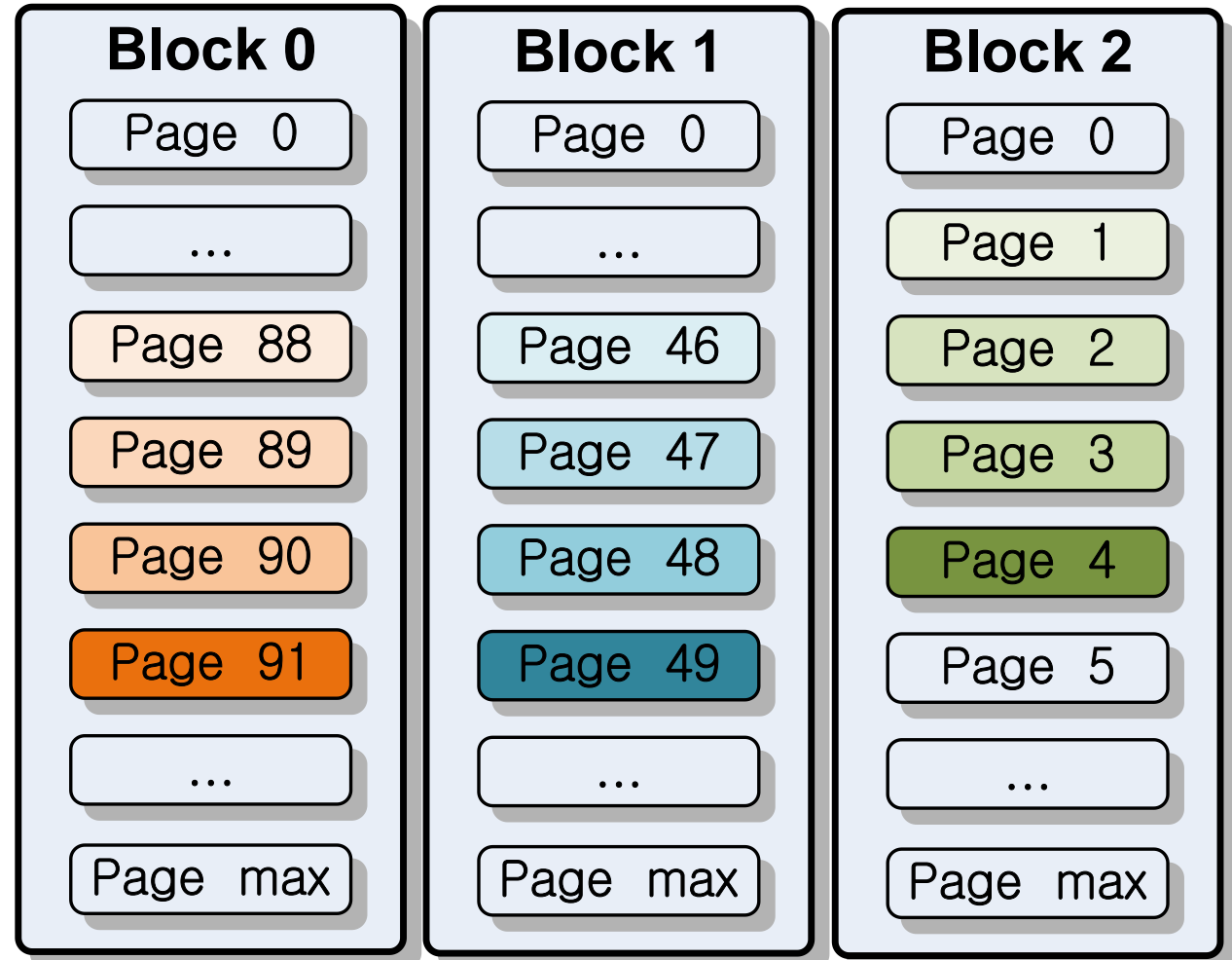


Mapping Technique and Data Overwriting

LPN



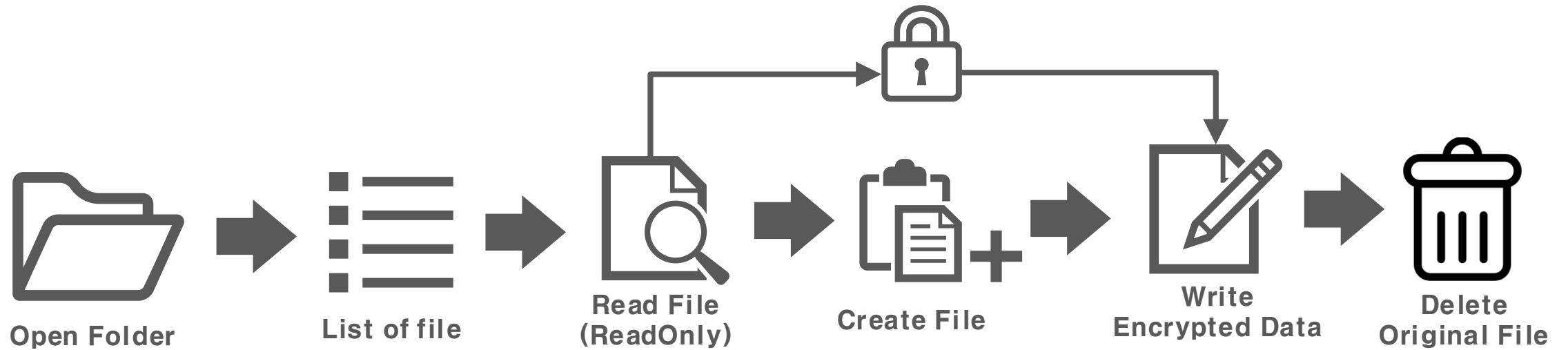
	Overwrite cnt=0	Overwrite cnt=1	Overwrite cnt=2	Overwrite cnt=3
LBA	LPN (Block, Offset)	LPN (Block, Offset)	LPN (Block, Offset)	LPN (Block, Offset)
43	(2,3)	(2,4)	(2,5)	(2,6)
72	(0,88)	(0,89)	(0,90)	(0,91)
84	(1,46)	(1,47)	(1,48)	(1,49)



Mapping Technique and Data Overwriting

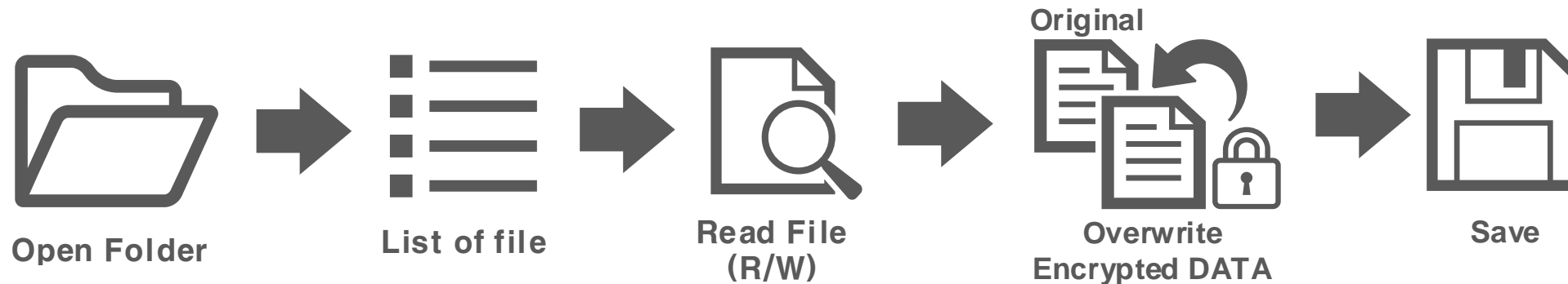


Type of Ransomware : Overwrite or Copy



Copy And Delete Type

Overwrite Type(In this time)



Steps : Overwritten Data Restoration



Locked File

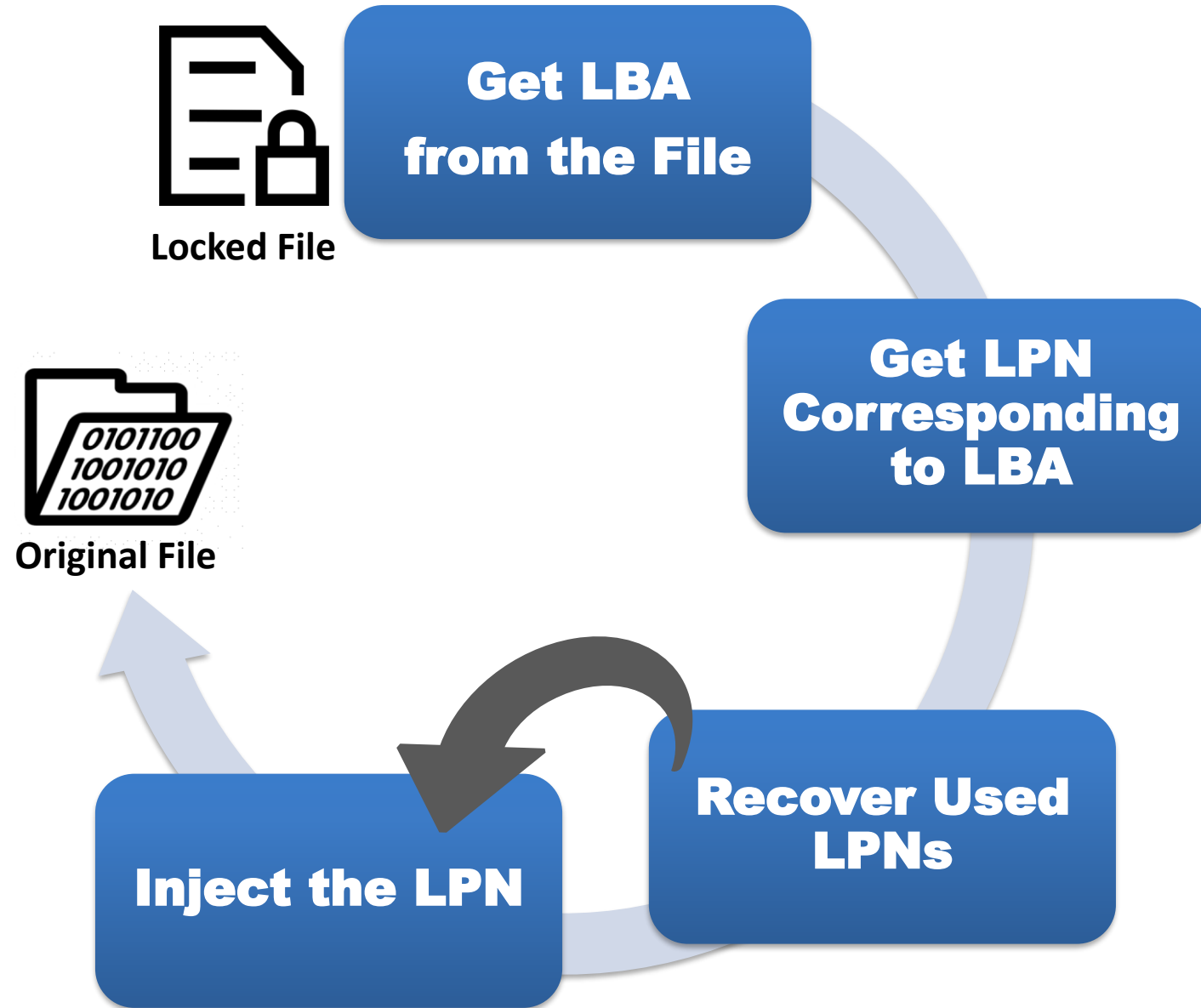
**Get LBA
from the File**

**Get LPN
Corresponding
to LBA**

**Recover Used
LPNs**

```
Menu
[B: SYSTEM | 65535 (#FFFF) sectors | ? helps |
000:0001 0004 E007 4040 0412 00FF FF1A AC10
010:0200 E853 0623 5359 5354 4540 2020 0101
020:2100 02FE 0001 5424 0000 0000 0000 0000
030:0000 0000 0000 0000 0000 0000 0000 0000
040:AE21 0400 2204 8598 8596 8692 8690 0900
050:8590 1865 9285 9809 3085 9165 9385 9909
060:0085 9E85 9F85 9685 9705 9280 8803 0593
070:8009 0320 F004 8504 20F0 0425 0409 FFD0
080:3009 0580 E202 0905 8DE3 0220 F004 8500
090:20F0 0485 A105 A0F0 1020 F004 38E5 A048
000:0820 F004 28E5 A185 A368 8502 2069 0520
0B0:8304 4C81 046C E002 6CE2 0209 0602 0580
0C0:4403 8E45 0309 0F80 4803 0909 8D42 0302
0D0:0020 56E4 40D4 0400 408C 8503 8D04 038E
0E0:0503 AD0A 0300 0803 F0D1 2059 E430 C060
0F0:0900 3503 8502 059E 059F F015 0000 819C
-----#003F-----
Sector: #0001 (1)      BPS: 512 (0/1)  Status: 1
Format: Sparta005    Type: 800T   Allocated: Yes
UTOC: #0002 (2)      Byte: #0000 (0)  Bit: 6
[+][+][+][+] to move cursor, [ESC] to exit
```


Steps : Overwritten Data Restoration



DEMO : Overwritten Data Restoration



What is Next?

- **Support for various SSDs.**
- **We need to Enhance our tool.**
- **Focus on Forensic tool for their needs.**
- **AES-XTS key extraction using side-channel attack.**
- **A study about Manage to keep Stale data Securely and Efficiently.**

Thank you!

If you have any question, please send me email



Kwonyoup Kim
CEO/founder
kkyoup@sntworks.kr



Seungjoon Lee
Senior Researcher
sj.lee@sntworks.kr



Twitter
[@SNTWORKS1](https://twitter.com/SNTWORKS1)



Youtube Channel
[SNTWORKS Inc.](https://www.youtube.com/SNTWORKS Inc.)



SNTWORKS