

DECEMBER 9-10 BRIEFINGS

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

Edda and and a state

#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
 - $\checkmark\,$ Offensive Security for Embedded Devices
 - $\checkmark\,$ Digital Forensics for Embedded Devices
 - $\checkmark\,$ Side Channel Attack & Fault Injection Attack with Reverse Engineering
 - ✓ Patent infringement Investigation





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?

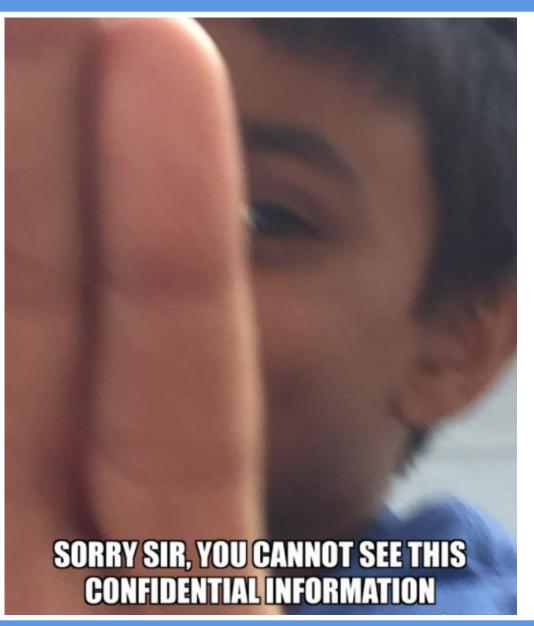
SSD Manufacturers

do not divulge information.

- SSD Controller manufacturers also do not divulge information.
- They protect their

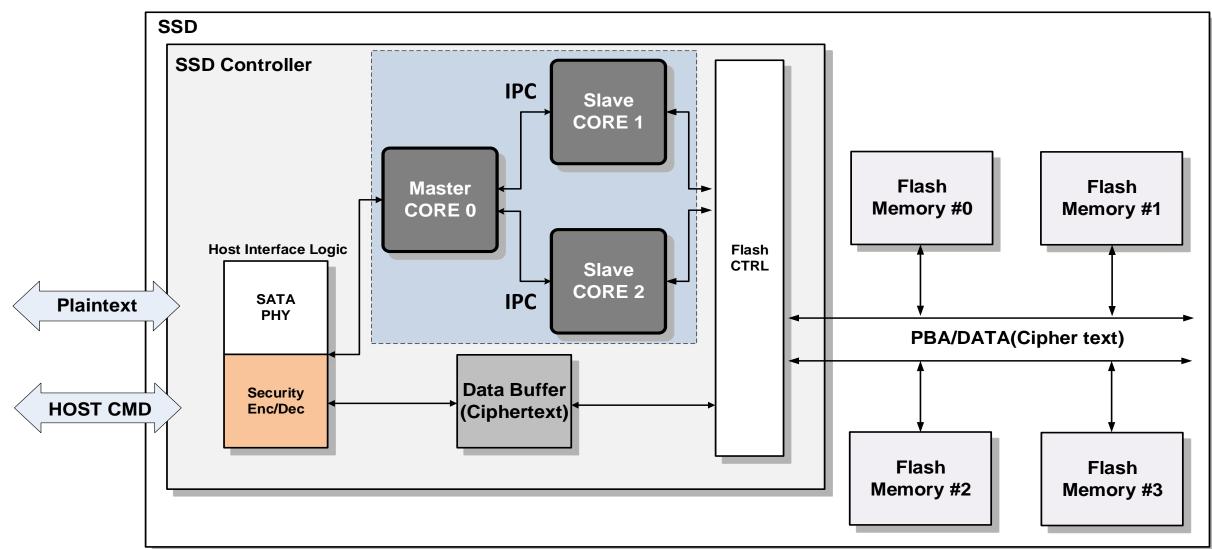
implementation details to protect their technologies.

No standards



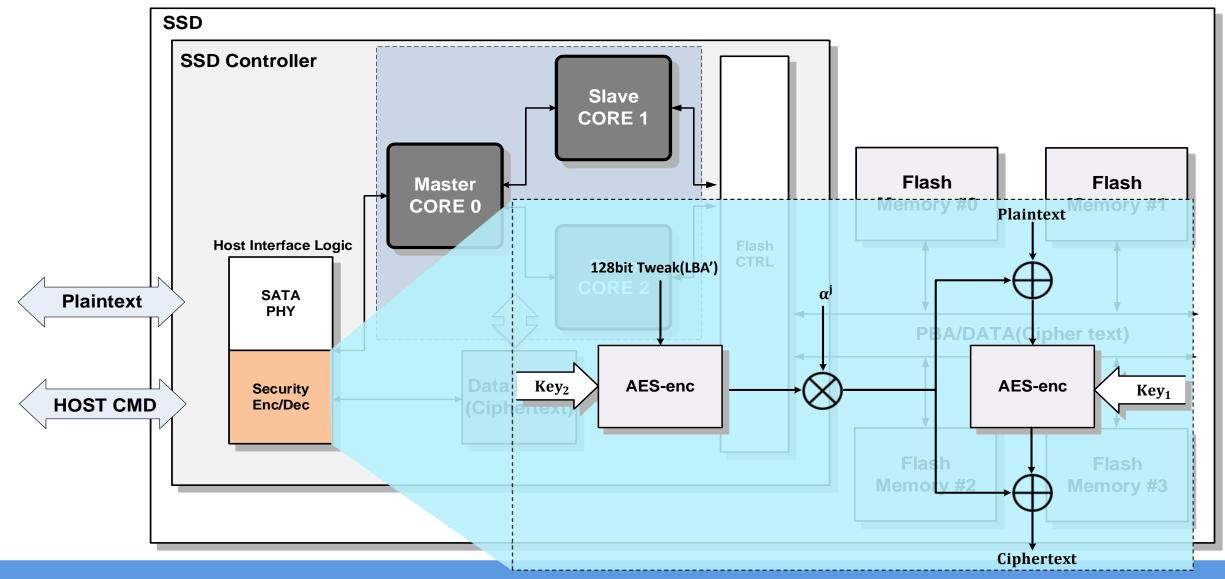
SSD Hardware Architecture

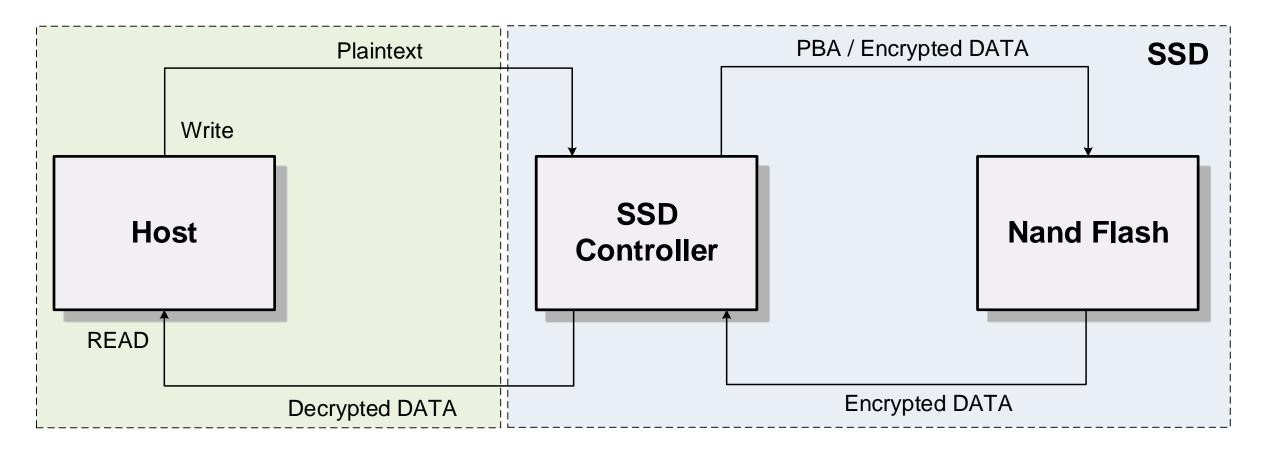
Multi Core based SSD Controller



SSD Hardware Architecture

AES-XTS





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.

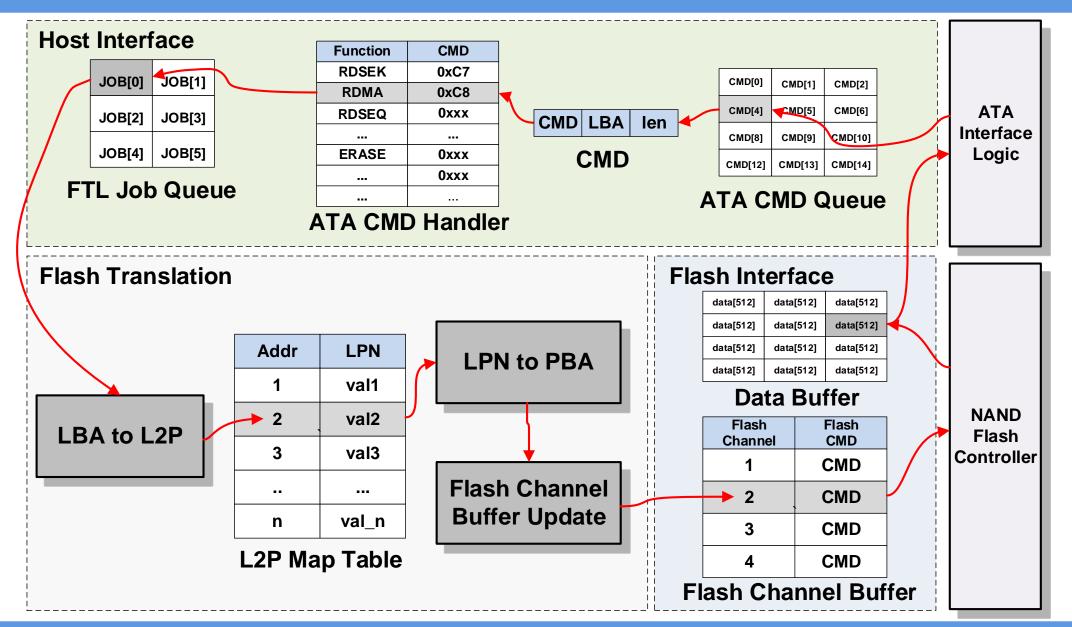
Security Encoding SSD Product information option ATA Interface Reproduction System Smart Store N Pay + Product order quantity: 1 AES DRAM Samsung SSD 850 PRO 128GB / MZ-7KE128B/KR Bull et Delivery Crypto Add/Change order conditions 95,000 KRW Engine CPU 11. 12. (Thu) 90% probability of arrival Compuzone Smart Store NPay + Product order quantity: 1 Flash Controller Micron Crucial MX500 Series 250GB TLC KRW 45,550 Add/Change order conditions NAND NAND NAND NAND 11. 12. (Thursday) 94% probability of arrival Flash Flash Flash Flash **Non-Security Encoding SSD** N Premium Shopping Mall Smart Store N Pay + Product order quantity: 1 ATA Interface TeamGroup GX2 (128GB) SSD hard HOT product 22,500 won Add/Change order conditions 11. 11.(Wed) 95% probability of arrival DRAM CPU Myssd Smart Store NPay + 322리뷰안 Product order quantity: 1 Review Announcement SSD 900G Blue 2.5 inch SATA 240GB Genuine Bulk Packaging Warranty 5 years 100550 Add/Change order conditions Flash Controller 32,800 KRW 36,300 11. 12. (Thu) 98% probability of arrival NAND NAND NAND NAND Delete selected product Wish selected product Flash Flash Flash Flash



SSD Firmware Reversing

Access All Physical Block

SSD Read Sequence Workflow



ATA CMD Queue

Host Interface Layer

ATA CMD: 0xC8(READ CMD)	SD:2000000 +0000000 0000000 00001459 00008000 NNNNNNNYFNNSNN SD:20000010 00000010 00000000 00000000 00000000 00004032 NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
	SD:20000040 00008027 0000000 E0A5A5A9 00000000 Tennicinni Addennini SD:2000050 00000000 00000000 00000000 C708F991 000000000 000000000 000000000 000000000 000000000 000000000 000000000 000000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 000000000 000000000 00
Sector Size(8bit) : 0x05	SD:20000090 00008EE0 0000000 0000009 8088483F 58000000000000000000000000000000000000
	SD:200000F0 00000014 0000000 00000000 00000000 © Ø
	SD:20000140 00000000 00000000 00000000 NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
LBA(24bit) : 0xE0A5A5A5	SD:20000180 00000000 0000000A 0000045A5 00000000 NNNNLNLNAANNNNNN SD:20000190 03020100 07060504 00000000 00000000 NSSEEEABNNNNNNNN SD:200001A0 E0A5A5A5 C8000000 00000005 80A5A5A5 355000008 NNNLNLNAANNNNNNNNNNNNNNNNNNNNNNNNNNNNN

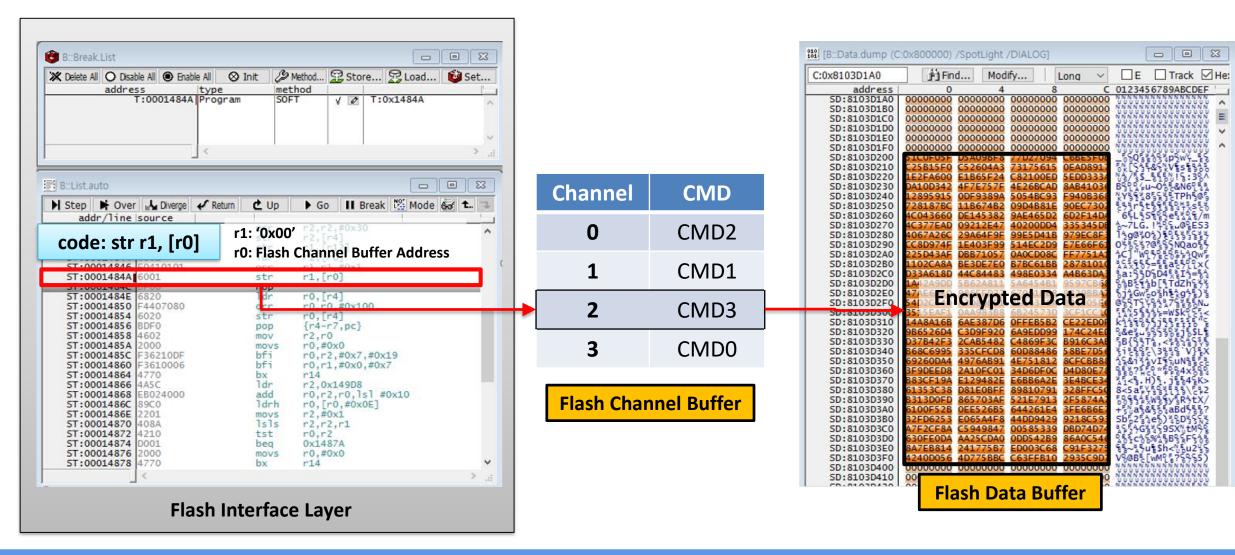
ATA CMD Handler

Host Interface Layer

Seg002:008085842 000 DC8 0 RDM: 0000C50C Sub_C50C Seg002:00808844 C4 DC8 0 RDM: 0000C514 B0 21 Seg002:00808844 C4 DC8 0 RDM: 0000C514 B1 10 DE5 LDR R1, R1, R1, LB1, LB12 Seg002:00808844 C4 DC6 L Seg002:00808514 B1 10 DE DE </th <th>lost Interface Layer</th> <th>ATA CMD H</th> <th>andler Table</th>	lost Interface Layer	ATA CMD H	andler Table
RNH:00000550C RNH:00000550C RNH:00000550C RNH:00000550C RNH:00000550C RNH:00000550C RNH:00000550C RNH:00000550C RNH:00000550C RNH:00000550C RNH:00000550C RNH:00000550C RNH:00000550C RNH:00000550C RNH:00000550C RNH:000005520 RNH:00005520 RNH:00005		seg002:00808B42 00	DCB 0
1001: 00000C5 0C sub_C5 0C 1001: 0000C5 1C 81 11 61 E0 1011: 0000C5 2C 00 E5 LD RR R11: R1,		seg002:00808B43 00	DCB 0
OH: 6000C5C0 Sub_C50C OH: 6000C50C Sub_C50C OH: 6000C50C Sub_C50C OH: 60000C50C Sub_C50C OH: 60000C50C Sub_C50C OH: 60000C50C Sub_C50C OH: 60000C50C Sub_C50C OH: 60000C510 Sub_C51D OH: 60000C52C OL 51D OH: 60000C52C OL 61C OH: 60000C52C OL 60C OH: 60000C52C OL 60		seg002:00808B44 C4	DCB 0xC4
0H:00000550C sub_C50C 0H:00000550C seg002:008088849 07 DCB 7 0H:00005510 03 10 DE 5 LDR R1, R0, H31 Seg002:00808884A 01 DCB 1 0H:00005510 03 10 DE 5 LDR R1, R0, H31 Seg002:00808884A 01 DCB 1 0H:00005510 B1 16 F5 LDR R2, F3ata_handler_table seg002:00808844 S5 DCCB DCC Sub_F3 0H:00005524 01 50 R1 R1, R1, R1, LSLH3 seg002:00808855 01 DCB 0 Seg002:00808855 00 DCB 0		seg002:00808B45 65 0B 01 00	DCD sub 1
0H:00000C50C F0 5F 20 E9 PUSH {RA-R12,LR} 0H:0000C514 80 10 00 E5 LDRB R1, [R0,#3] 0H:0000C514 8C 21 9F E5 LDR R1, [R0,#3] 0H:0000C514 8C 21 9F E5 LDR R2, [ssta handler_table 0H:0000C514 8C 21 9F E5 LDR R4, [M007_H2943 0H:0000C520 02 50 81 E0 ADD R5, R1, R2 0H:0000C520 02 50 81 E0 ADD R5, R1, R2 0H:0000C520 02 50 81 E0 ADD R5, R1, R2 0H:0000C520 02 50 81 E0 ADD R5, R1, R2 0H:0000C520 02 50 81 E0 ADD R5, R1, R2 0H:0000C520 00 51 E3 CMP R1, [R5, #1] 0H:0000C520 00 00 51 E3 CMP R1, #0, #10 0H:0000C520 01 00 AD BEQ 10c_C688 0H:0000C50 01 00 AD BEQ 10c_C688 0H:0000C50 01 00 AD BEQ 10c_C688 0H:0000C50 01 00 AD BEQ 10c_C50 0H:0000C50 01 00 AD BEQ 10c_C50 0H:0000C50 01 00 AD BEQ R2, [R5,#1] 0H:0000C50 01 00		0	
0H: 0000C510 03 10 D0 E5 LDRB R1, [R0,H3] 0H: 0000C510 021 9F E5 LDR R2, [sata_handler_table 0H: 0000C510 01 11 61 E6 R2 Seg002:00808848 C5 DC6 02C 0H: 0000C510 01 11 61 E0 RS R1, R1, R1, R1, LSL#3 Seg002:00808850 06 DC6 DC8 6 0H: 0000C524 01 05 E5 LDR R1, R2, R1 R1, R2 Seg002:00808851 01 DC8 0 Seg002:00808852 C6 DC8 DC8 DC8 DC8 0 Seg002:00808857 00 DC8 DC8 DC8 DC8 0 Seg002:00808857 00 DC8 0 Seg002:00808856 DC8 DC8 0 Seg002:00808856 DC8 DC8 0 Seg002:00808856 DC8 DC8 0 Seg002:00808856 DC8 DC8 0 Seg002:00808857 00 DC8 0 Seg002:00808856 DC2 DC8 0 Seg002:00808856 DC2 DC8	:0000C50C F0 5F 2D E9 PUSH {R4-R12,LR}		
DM: 000005514 8C 21 9F E5 LDR R2, Fsata handler_table DM: 00000516 81 11 61 E0 R50 DCC sub F1 000: 000005510 81 11 61 E0 R50 R1, R1, R1, R1, LSL83 Seg002:00808842 78 F5 00 00 DCC sub F1 001: 000005220 02 50 81 E0 ADD R5, R1, R2 Seg002:00808852 C6 DCE sub F1 001: 000005220 01 00 95 E5 LDR R1, R1, R1, LSL83 Seg002:00808852 C6 DCE sub F1 001: 000005220 01 00 90 51 E3 CMP R1, R1, #1 Seg002:00808852 C6 DCE sub F1 001: 000005230 54 00 00 00 ABEQ loc_C688 Seg002:00808852 C6 DCE sub F1 001: 00000550 01 00 00 00 ABEQ loc_C500 Seg002:00808855 00 DCE sub F1 001: 00000500 01 20 95 E5 LDR R2, [R5,#1] Seg002:00808856 01 DCB 0 Seg002:00808856 01 20 95 E5 LDR R2, [R5,#1] Seg002:00808856 01 DCB 0 Seg002:00808856 01 20 95 E5 LDR R2, [R5,#1] Seg002:00808866 C8 DCE 0/2 0/2 0/2 0/2 0/2 0/2 0/2 0/2 0/2 0/2	:0000C510 03 10 D0 E5 LDRB R1, [R0,#3]		
UNI: 000005518 At 1 97 E5 LDR R4, #1, R1, R1, L1, L143 UNI: 000005216 B1 16 E8 R1, R1, R1, R1, L1, L143 UNI: 00000528 0.6 B5 LDR R1, R1, R1, R5, H1] DCB Seg002:00808852 C6 DCB DCB 1 UNI: 00000528 D4 L4 E1 LDRD R6, R7, R1, R2 R4, #0x14] Seg002:00808852 C6 DCB DCB 0 UNI: 00000528 D4 D4 BEQ Loc_C688 DCB DCB 0 Seg002:00808853 D7 08 08 0 DCB 0 Seg002:00808856 DC 00 DCB 0<	:0000C514 8C 21 9F E5 LDR R2, =sata_handler_table	U	
Num. 000005250 02 50 N1 for N1,			
Sub: 000005224 0f 10 05 E5 LDR R1, [R5, #1] SUD: 000005228 04 61 C4 E1 LDRD R6, R7, [R4, #0x14] SUD: 00000522 04 61 C4 E1 LDRD R6, R7, [R4, #0x14] SUD: 00000522 04 61 C4 E1 LDRD R6, R7, [R4, #0x14] SUD: 00000522 04 61 C4 E1 LDRD R6, R7, [R4, #0x14] SUD: 00000522 04 61 C4 E1 LDRD R6, R7, [R4, #0x14] SUD: 00000520 05 54 00 00 51 E3 CMP R1, #0 SUD: 00000520 10c_C688 Seg002:00808853 07 08 00 80 Sub: 0000550 10c_C500 Seg002:00808855 00 SUD: 00000550 10c_C500 Seg002:00808856 00 Sub: 00000550 10c_C500 Seg002:00808856 01 Sub: 00000550 10c_C500 Seg002:00808856 01 Sub: 00000550 10c_C500 Seg002:00808856 01 Seg002:00808856 01 Seg002:00808856 01 Seg002:00808856 01 Seg002:00808866 01 Seg002:00808866 01 Seg002:00808866 01 Seg002:00808860 01 Seg002:00808866 01 Seg002:00808860 01 Seg02:00808866 01 Seg002:00808860 01 Seg02:00808866 01			
R0M: 00000C528 D4 61 C4 E1 LDRD R6, R7, [R4, #0x14] R0M: 00000C528 D4 61 C4 E1 LDRD R6, R7, [R4, #0x14] R0M: 00000C528 054 00 00 51 E3 CMP R1, #0 R0M: 00000C530 54 00 00 00 REQ loc_C688 R0M: 00000C520 00008855 00 DCE 00 R0M: 00000C50 00 Seg002:00808855 00 DCE 00 R0M: 00000C50 00 Ioc_C500 R0M: 00000C50 01 Ioc_C500 R0M: 00000C50 01 Ioc_C500 R0M: 00000C50 01 Ioc_C500 R0M: 00000C50 01 R2, [R5, #1] R0M: 00000C50 01 Ioc_C500 R0M: 00000C50 01 R2, [R5, #1] R0M: 00000C50 01 Ioc_C500 R0M: 00000C50 01 R2, [R5, #1] R0M: 00000C50 01 Ioc_C500 R0M: 00000C50 01 R0, R0, R0 R0M: 00000C50 01 R0, R0, R1 R0M: 00000C50 01 R0, R0, R0 R0M: 00000C50 01 R0, R0, R1 R0M: 00000C50 01 R0, R0, R1 R0M: 0000C500 01 R0, R0, R1 <tr< td=""><td></td><td></td><td></td></tr<>			
R0H:00000C52C 00 00 51 E3 CMP R1, #0 R0H:00000C530 54 00 00 0A BEQ loc_C688 R0H:00000C530 54 00 00 0A BEQ loc_C688 seg002:00808855 00 DCB 0 seg002:00808855 01 DCB 1 seg002:00808856 01 DCB 1 seg002:00808866 01 DCB 0xC9 seg002:00808868 C01 DCB 1 seg002:00808868 C01 DCB 1 <td></td> <td></td> <td></td>			
ROM: 00000C530 54 00 00 0A BEQ loc_C688 DCB 0 seg002:000008550 00 DCB 0 seg002:000008550 01 DCB 0 seg002:000008550 01 DCB 0 seg002:000008550 01 DCB 0 seg002:000008856 01 DCB 1 seg002:000008856 01 DCB 1 seg002:000008550 01 DCB 1 seg002:0000088650 01			
Seg002:00808555 00 DCB 0 Seg002:00808558 00 DCB 0 Seg002:00808558 00 DCB 0 Seg002:00808556 00 DCB 0 Seg002:00808857 00 DCB 0 Seg002:00808856 00 DCB 0 Seg002:00808856 00 DCB 0 Seg002:00808856 00 DCB 0 Seg002:00808856 01 DCB 0 Seg002:00808856 01 DCB 0 Seg002:00808860 C8 DCB 0XC8 Seg002:00808860 C9 DCB 0XC9 Seg002:00808866 C91 DCB 0XC9 Seg002:00808866 C91 DCB 0XC8 Seg002:00808860 C1 DCB 1 DCB 0XC9 Seg002:00808860 01 DCB 1 Seg002:00808860 01 DCB 1 DCB 0XC9 Seg002:00808860 01 DCB 1 Seg002:00808860 01 DCB 1 DCB 0XC4	· · · · · · · · · · · · · · · · · · ·		
Seg002:0080885A BD CC 00 00 DCD sub_CC Seg002:0080885E 00 DCB 0 Seg002:00808860 C8 DCB 0 Seg002:00808860 C9 DCB 1 Seg002:00808866 C9 DCB 0xC9 Seg002:00808868 AC 03 01 00 DCD RDMA F Seg002:00808868 AC 03 01 00 DCD RDMA F Seg002:00808866 C01 DCB 1 Seg002:00808866 C01 DCB 1 Seg002:00808860 01 DCB 1 Seg002:00808860 01 DCB 1 Seg002:00808866 01 DCB 1 Seg002:00808866 CA DCB 0xC4	.0000C330 54 00 00 0H DEQ 10C_C088	0	
Seg002:0080885E 00 DCB 0 Seg002:0080885F 00 DCB 0 Seg002:0080885F 00 DCB 0 Seg002:00808860 C8 DCB 0 Seg002:00808860 C8 DCB 0 Seg002:00808860 C8 DCB 0 Seg002:00808861 AC 03 01 00 DCB 1 IOM:0000055C0 01 20 95 E5 LDR R2, [R5,#1] Seg002:00808861 AC 03 01 00 DCB 1 IOM:0000055C0 81 20 95 E1 LDRH R1, [R5,#5] IOM:0000055C0 91 00 50 E3 CMP R0, #0 R0M:0000055C0 91 00 50 E3 CMP R0, #1 Seg002:00808867 C9 DCB 0xC9 Seg002:00808868 AC 03 01 00 DCD R0MA H Seg002:00808866 01 DCB 1 Seg002:00808860 01 DCB 1 Seg002:00808860 01 DCB 1 Seg002:00808860 01 DCB 1 Seg002:00808866 01 DCB 1 Seg002:00808866 CA DCB 0xCA		seg002:00808B59 00	DCB Ø
Seg002:0080885F 00 DCB 0 0M:0000055C0 loc_C5C0 Seg002:00808860 C8 DCB 0X 0M:0000055C0 loc_C5C0 Seg002:00808861 AC 03 01 00 DEB 0 0M:0000055C0 loc_C5C0 Seg002:00808861 AC 03 01 00 DEB 0 0M:0000055C0 120 95 E5 LDR R2, [R5,#1] DCB 1 DCB 0		seg002:00808B5A BD CC 00 00	DCD_sub_C
Image: Seg002:00808860 C8 DCB 0xC8 DM:0000C5C0 loc_C5C0 DM:0000C5C0 loc_C6C0 DM:0000C5C0 loc_C6C0 DM:0000C5C0 loc_C6C0 DM:0000C5D0 loc_C6C0 BS loc_C7 DM:0000C5D0 loc_C6C0 BS loc_C6C0 BS loc_C6C0 <td></td> <td>seg002:00808B5E 00</td> <td>DCB Ø</td>		seg002:00808B5E 00	DCB Ø
OM:0000055C0 loc_C5C0 OM:0000055C0 loc_C9 OM:0000055C0 loc_D0 OM:0000055D0 loe_A0 OM:0000055D4 loe_A0 OM:0000055D8 B5 OM:0000055D8 loc_D0 DS loc_B OM:0000055D8 loc_D0 DS loc_B OM:0000055D0 loc_L02 OM:0000055D0 loc_L02 OM:0000055D0 loc_L02 OM:0000055D0 loc_L02 OM:0		seg002:00808B5F 00	DCB 0
0M:0000C5C0 loc_C5C0 0M:0000C5C0 loc_C5C0 0M:0000C5C0 120 0M:0000C5D0 120		seg002:00808B60 C8	DCB 0xC8
R0M:00000C5C0 1 oc_C5C0 R0M:00000C5C0 01 20 95 E5 LDR R2, [R5,#1] R0M:00000C5C4 B5 10 D5 E1 LDRH R1, [R5,#5] R0M:00000C5C8 32 FF 2F E1 BLX R2 R0M:00000C5C0 01 00 40 03 MOVEQ R0, #0 R0M:00000C5C4 85 00 05 E1 LDRH R0, #0 R0M:00000C5C8 32 FF 2F E1 BLX R2 R0M:00000C5C0 00 00 50 E3 CMP R0, #0 R0M:00000C5C0 01 00 A0 03 MOVEQ R0, #1 R0M:00000C5D4 04 00 C4 05 STRBEQ R0, [R4,#(byte_1A29C - 0x1A298)] R0M:00000C5D8 B5 00 D5 E1 LDRH R0, [R5,#5] R0M:00000C5D0 01 00 10 E3 TST R0, #0x100		seg002:00808B61 AC 03 01 00	DIC RDMA
R0M:0000C5C0 01 20 95 E5 LDR R2, [R5,#1] seg002:0080666 01 DCB 1 R0M:0000C5C0 85 10 D5 E1 LDRH R1. [R5,#5] DCB 02 R0M:0000C5C0 32 FF 2F E1 BLX R2 Seg002:008088867 C9 DCB 02	0000C5C0 loc_C5C0		
R0M:000005526 32 FF 2F E1 BLX R2 Seg002:00808B67 C9 DCB 0xC9 R0M:000005506 01 00 A0 03 MOUEQ R0, #0 seg002:00808B68 AC 03 01 00 DCD RDMA_F R0M:000005506 01 00 A0 03 MOUEQ R0, #1 seg002:00808B68 AC 03 01 00 DCB 1 R0M:000005504 04 00 C4 05 STRBEQ R0, [R4,#(byte_1A29C - 0x1A298)] seg002:00808B6C 01 DCB 1 R0M:000005506 01 0C 10 E3 TST R0, #0x100 DCB 1 seg002:00808B6D 01 DCB 1 R0M:000005506 01 0C 10 E3 TST R0, #0x100 DCB 1 seg002:00808B6E CA DCB 0xCA			DCB 1
ROM:00000500 02 11 21 21 21 21 21 21 21 21 21 21 21 21			DCB 0xC9
ROM:0000C5D0 01 00 03 MOUEQ R0, #1 ROM:0000C5D4 04 00 C4 05 STRBEQ R0, [R4,#(byte_1A29C - 0x1A298)] seg002:0080886C 01 DCB 1 ROM:0000C5D8 B5 00 D5 E1 LDRH R0, [R5,#5] seg002:0080886D 01 DCB 1 ROM:0000C5DC 01 0C 10 E3 TST R0, #0x100 DCB 0CB 0CB<			
R0M:0000C5D4 04 00 C4 05 STRBEQ R0, [R4,#(byte_1A29C - 0x1A298)] R0M:0000C5D8 85 00 D5 E1 LDRH R0, [R5,#5] R0M:0000C5DC 01 0C 10 E3 TST R0, #0x100 DCB_0xCA DCB_0xCA	0000C5D0 01 00 A0 03 MOVEQ R0, #1	0	
ION:0000C5DC 01 0C 10 E3 TST R0, #0x100 DCB_0xCA			
seguaz:0000000r /o r5 00 00 DCL sub_r:			
	100_0000	268007:0000000L 10 LD 00 00	

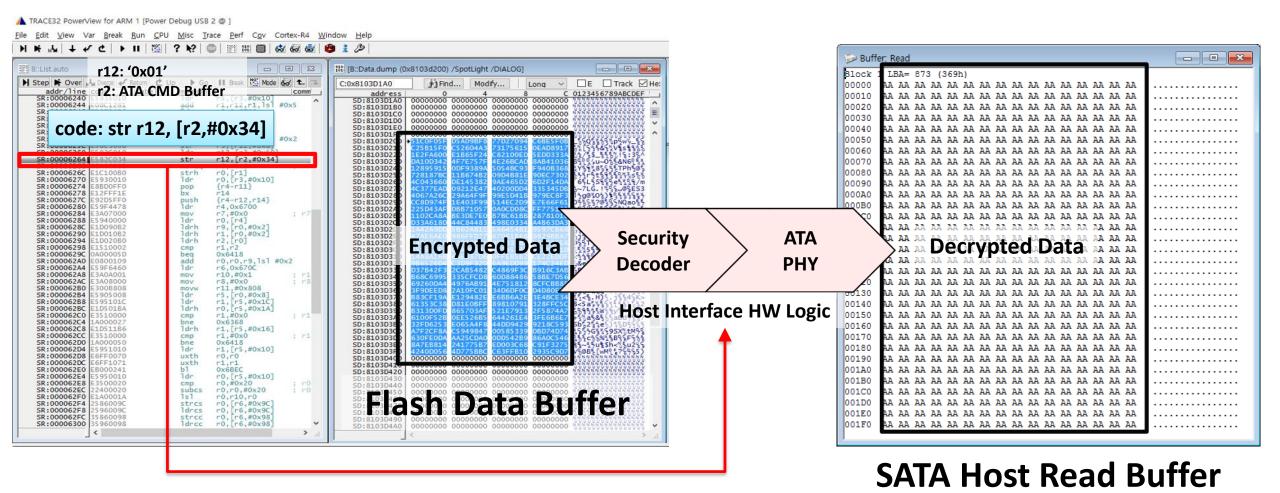
Flash Chip → Flash DATA Buffer []

Flash Interface Layer → Flash Chip → Flash Interface Layer



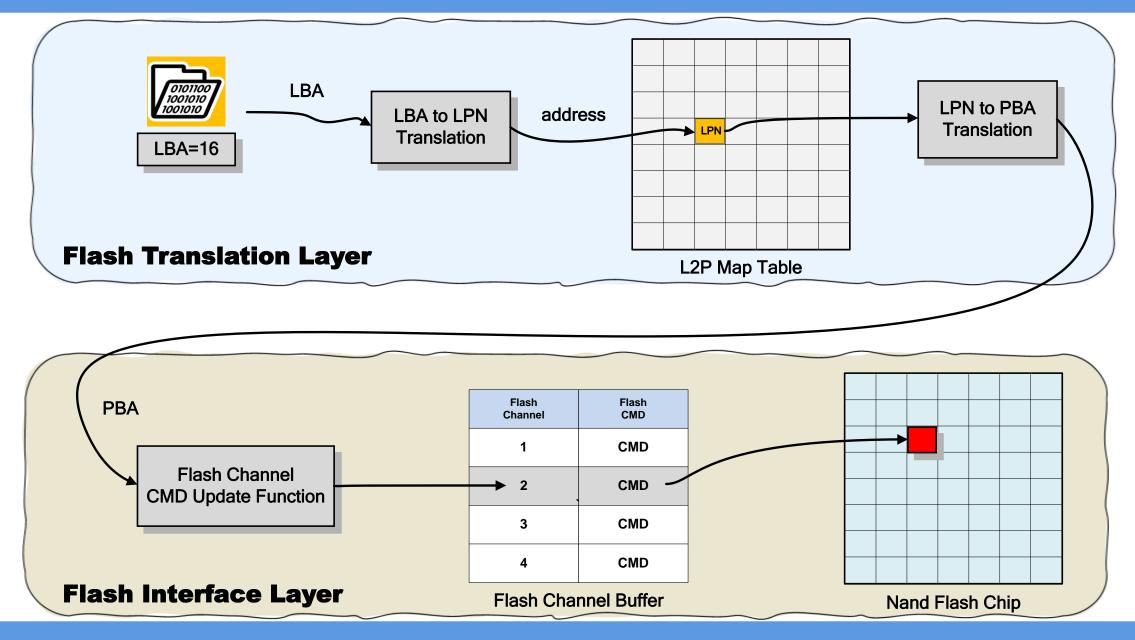
Flash Data Buffer [] → Host Interface Logic

Flash Interface Layer → Host Interface Layer → Host PC



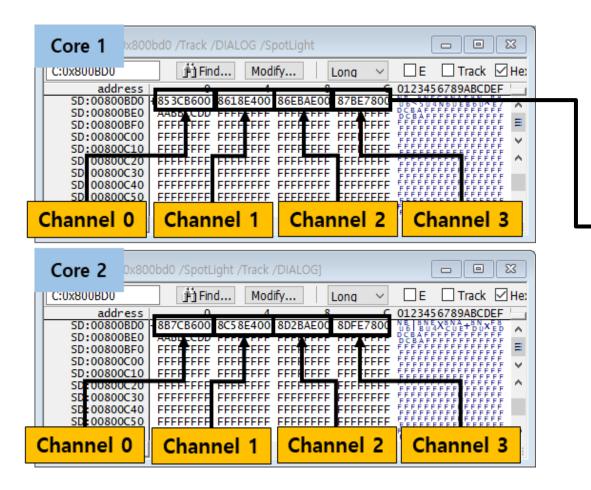
18

Figure Out Where PBA and Channel Buffer are



L2P Map Table

Flash Translation Layer

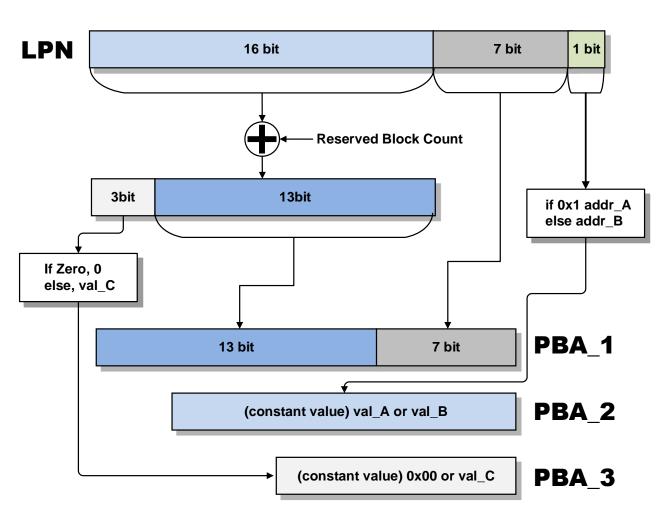


0101 [B::d.dump 0x8b	8a0000 /Spo	otLight]			
address	0	4	8		0123456789ABCDEF
SD:8B88C760	03B63303	3203CB3E	CB3F03CB	03CB3303	^E 3 ^B E> ^C E2 ^C E2 ^C E3 ^C E3 ^C E > '#4 ⁹ 4 ^S ? '#5 ⁹ 4 ^S ≥ ^B #4
SD:8B88C770	3423603E	603F0394		34238D3E	$> #4^{9}_{4x}? #5^{9}_{4x}>_{0}#4$
SD:8B88C780	8D3F0355	03553523	3423863E	863F03B6	Ux?p#5Ux>6#46x?6
SD:8B88C790	03B63523	3423CB3E	CB3F03CB	03CB3523	#58525#46526#565 @426424742742@U26
SD:8B88C7A0	36039440	94410394		36035540	
SD:8B88C7B0	55410355	03553703	3603B640	B64103B6	U vAU v/ U ve k vO k vA k
SD:8B88C7C0	03B6370			3CB3703	E7BE@CE6CEACE7CE
SD:8B88C7D0	3823604	Using	g Area	8238D40	@`#8 ⁹ EA`#9 ⁹ E@8#8
SD:8B88C7E0	8D41039	20220040	CR4102CR	64103B6	
SD:8B88C7F0 SD:8B88C800	03B63923 3A039442	94430394	CB4103CB 03943B03	03CB3923 3A035542	#96X@B#8CEACB#9CE
SD:8888C810	55430355	03553B03	3C03B642	8D430355	B ⁹ E ⁹ EC ⁹ E ⁹ E ⁸ E ⁹ E ⁸ E ¹
SD:8888C820	03553D23	3A238642	B64303B6	03B63B03	U _X CU _X ; U _X B _{6X} <u<sub>XC_D +-UEP8 + BECBE BE</u<sub>
SD:8888C830	3A03CB42	CB4303CB	03CB3B03	3C236042	B_{P}^{CE} ;
SD:8888C840	60430394	03943D23	FF238D42	FFFFFFFF	YEC' #_YER8 #FFFFF
SD:8888C850	FFFFFFFF	FEFEFEFE	FFFFFFFF	FFFFFFFF	FFFFFFFFFFFFFFF
SD:8888C860	FFFFFFF	CECEEEEE	CECEEEEE	FFFFFFF	FFFFFFFFFFFFFFF
SD:8888C870	FFFFFFF	CECEEEEE	CECEEEEE	FFFFFFF	FFFFFFFFFFFFFF
SD:8B88C880	FFFFFFF	FFFFFFFF	FFFFFFFF	FFFFFFF	FFFFFFFFFFFFFFFF
SD:8B88C890	FFFFFFF	FFFFFFFF	FFFFFFFF	FEFEFFFF	FFFFFFFFFFFFFFF
SD:8888C8A0	FFFFFFF	FFFFFFFF	FFFFFFFF	FFFFFFFF	FFFFFFFFFFFFFFF FFFFFFFFFFFFFFF FFFFFFF
SD:8B88C8B0	FFFFFFF	FFFFFFF	FFFFFFF	FFFFFFF	FFFFFFFFFFFFFFF
SD:8B88C8C0	FFFFFFF	FFFFFFF	FFFFFFF	FFFFFFF	FFFFFFFFFFFFFFF
SD:8B88C8D0	FFFFFFF	FFFFFFF	FFFFFFF	FFFFFFF	FFFFFFFFFFFFFF
SD:8B88C8E0	FFFFFFF	FFFFFFF	FFFFFFF	FFFFFFF	FFFFFFFFFFFFFFF
SD:8B88C8F0	FFFFFFF	FFFFFFF	FFFFFFF	FFFFFFF	FFFFFFFFFFFFFFFF
SD:8B88C900	FFFFFFF	FFFFFFF	FFFFFFF	FFFFFFF	FFFFFFFFFFFFFFFF
SD:8B88C910	FFFFFF			FFFFFF	ÉÉÉÉÉÉÉÉÉÉÉÉÉÉÉÉ FFFFFFFFFFFFFFF
SD:8B88C920	FFFFFF	Empty	/ AREA	FFFFFF	FFFFFFFFFFFFFFFFF
SD:8B88C930	FFFFFF			FFFFFFF	FFFFFFFFFFFFFFFF
	<				ي <

LPN -> PBA Translation

Flash Translation Layer

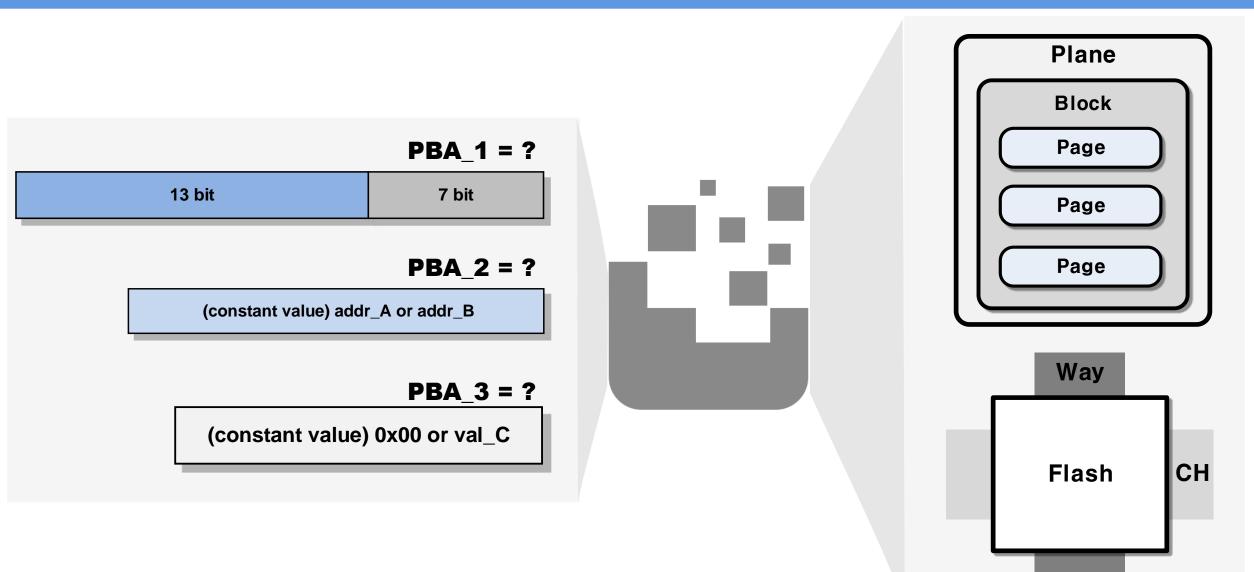
	🔲 🛃 🖼			
	ROH:800077D8 ROM:800077D8 ROH:800077D8 PBA_calc1 ROH:800077D8 PBA_calc1 ROH:800077D8 PB5 ROH:800077D8 PB5 ROH:800077D8 PB5 ROH:800077D8 PB5 ROH:800077D8 PB5 ROH:800077D8 PB5 ROH:800077D4 PC A87 ROH:800077D4 PC A87	{R4- <mark>R6</mark> ,LR} R6, R0 R0, #0x7A8		
 [🖌 🖼			
ROM	:0000286C CB 4B	LDR	R3, =channel_count	
ROM	:0000286E CE 4D	LDR	R5, =dword_1C7E8	
ROM	:00002870 11 6A	LDR	R1, [R2,#0×20]	
ROM	:00002872 9C 6C	LDR	R4, [R3,#(dword_1C71	· · ·
	:00002874 D5 F8 E0 51		R5, [R5,#(dword_1C9C	
1 13	:00002878 DF 6C	LDR	R7, [R3,#(dword_1C71	C - 0x1C6D0)]
:000 KOM	:0000287A 21 FA 04 F4		R4, R1, R4	
	:0000287E 66 19 :00002880 D3 F8 B4 50	ADDS	R6, R4, R5	4 0+100001
	:00002880 D3 F8 B4 50 :00002884 5B 6C	LDR.W	R5, [R3,#(dword_1C78 R3, [R3,#(dword 1C71	/ 4
	:00002886 26 FA 05 F4		R4, R6, R5	4 - 0XIC000)]
	:00002888 AF 40	LSLS	R7, R5	
	:0000288C 7F 1E	SUBS	R7, R7, #1	
ROM	:0000288E 5B 1E	SUBS	R3, R3, #1	
ROM	:0			
ROM	ROM:00014858			
ROM	:0ROM:00014858			
ROM	:0 ROM:00014858			
ROM	^{:0} ROM:00014858		sub 14858	
ROM	*0 ROM · 00014858 0	2 46	MOV	R2, RØ
ROM	ROM:0001485A		MOVS	R0, #0
	:0 ROM:0001485C			R0, R2, #7, #0x19
				· · ·
	* ROM:00014860			R0, R1, #0, #7
NOP	^{:0} ROM:00014864 7	0 47	BX	LR
	ROM:00014864		; End of function	on sub_14858
	ROM:00014864			



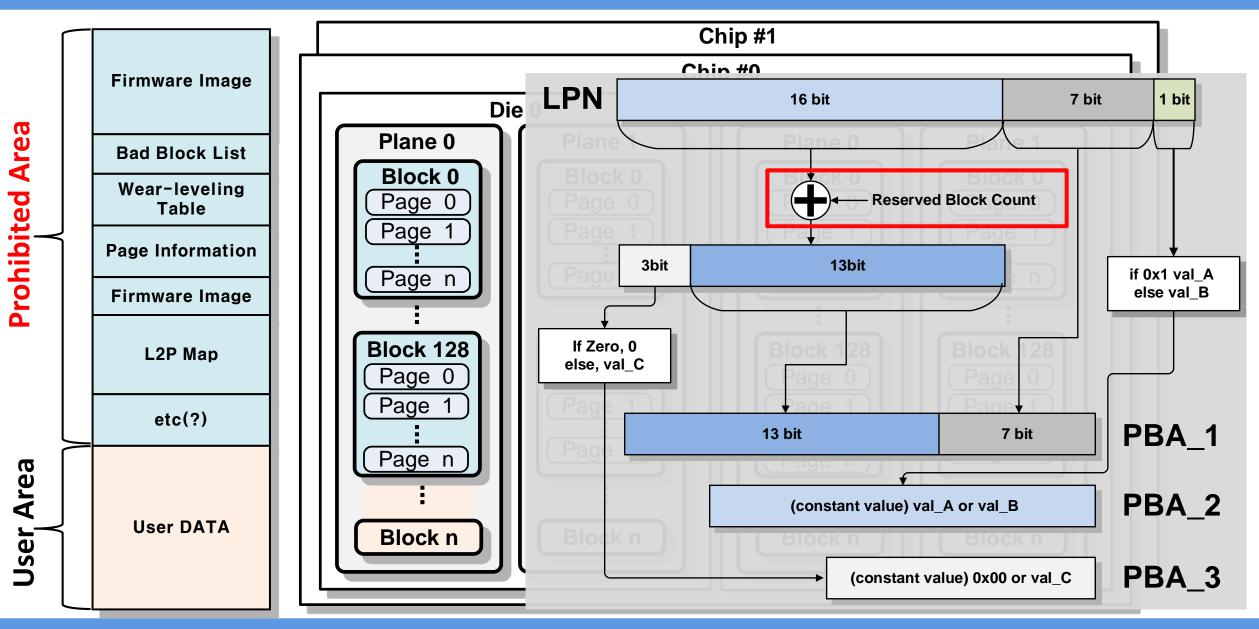
Logical Expression

Raw Code

LPN -> PBA Translation



LPN -> PBA Translation (Reserved Block Count)



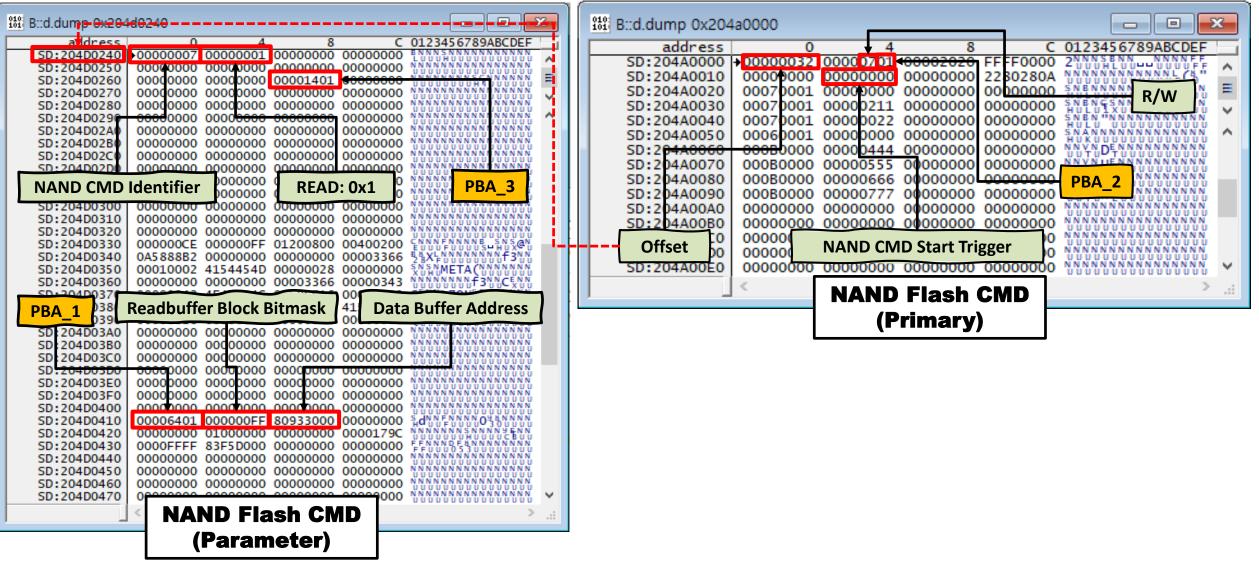
Flash Channel Buffer

Flash Interface Layer

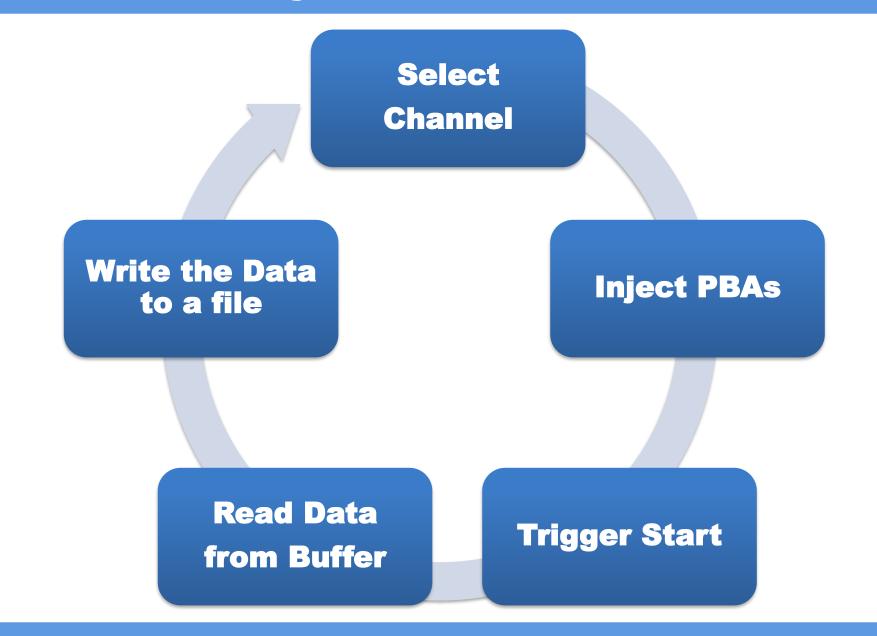
TRACE32 PowerView for ARM 3 [Power Debug USB 2 @] Eile Edit View Var Break Run CPU Misc Trace Perf Cov Corte Channel 0							
File Edit View Var Break Run CPU Misc Irac ▶ ▶ ▶ ■ ▶ ■ ₩ ↓ ✓ ₾ ▶ ■ ₩ ↓ ∅ ? № □ <t< td=""><td></td><td>Channel I</td><td>Channel 2</td><td></td></t<>		Channel I	Channel 2				
B::List.auto		뱳 B::Data.dump (0x20490000) /NoAscii /DIALOG 🗖 🗉 🖾	: B::Data.dump (0x204A0000) /NoAscii /SpotLig 🗖 🔳 🖾	뱺 B::Data.dump (0x204B0000) /NoAscii /DIALOG 🗖 🔲 🖾			
H H L C L H II 12 6 L - A	C:0x20480000	C:0x20490000	C:0x204A0000	C:0x204B0000			
ST:00014828 D401 ST:0001482A F0410101 orr	address 0 4 8 C SD:20480000 +00000032 00000601 00022222 FFFF0000 A SD:20480010 00000000 00000000 0280280A A	address 0 4 8 C 5D:20490000 +00000031 00000601 0001111 FFFF000 5D:20490010 0000000 0000000 0000000 2280280A	SD:204A0000 00000033 00000701 00013131 FFFF0000 SD:204A0010 0000000 00000000 00000000 2280280A	address 0 4 8 C SD:20480000 +0000033 0000601 0003333 FFFC000 SD:20480010 0000000 00000000 00000000 2280280A			
ST:0001482E 2820 cmp ST:00014830 D003 beq ST:00014832 EA414183 orr	5D:20480020 00660001 0000000 0000000 00000000 5D:20480030 00070001 00000011 00000000 00000000	SD:20490020 00070001 00000200 0000000 00000000 SD:20490030 00060001 00000011 00000000 00000000	SD:204A0020 0066001 0000000 0000000 0000000 SD:204A0030 0007001 00000011 0000000 0000000 SD:204A0040 0066001 0000022 0000000 00000000	SD:204B0020 00060001 00000213 0000000 00000000 E SD:204B0030 00060001 00000011 00000000 00000000 U			
ST:00014832 EA414183 orr ST:00014836 F4410180 orr ST:0001483A F0420230 orr	SD:20480040 00060001 00000022 00000000 00000000 SD:20480060 00000000 00000000 00000000 00000000	SD:20490040 00060001 00000233 0000000 00000000 SD:20490050 00460001 00000033 0000000 00000000 ^ SD:20490060 0000000 00000000 00000000 0000000	SD:204A0050 00070001 00000033 00000000 00000000 SD:204A0060 00000000 00000000 00000000 00000000	SD:20480040 0007001 0000022 0000000 0000000 SD:20480050 0006001 00000033 00000000 0000000 SD:20480060 000000 0000000 00000000 00000000			
ST:0001483E 6022 str ST:00014840 F8CC1000 str ST:00014844 F8CC1000 ldr	SD:20480070 0000000 0000000 0000000 0000000 SD:20480080 0000000 0000000 00000000 00000000	SD:20490070 0000000 0000000 0000000 0000000 SD:20490080 0000000 0000000 0000000 0000000	50-20440070	SD:204B0070 0000000 0000000 0000000 0000000 SD:204B0080 0000000 0000000 00000000 00000000			
ST:00014846 F0410101 orr ST:0001484A 6001 str	SD:20480090 00000000 00000000 00000000 00000000 00000000 SD:204800A0 00000000 00000000 00000000 SD:204800B0 00000000	SD:20490090 00000000 00000000 00000000 00000000 SD:204900A0 00000000 00000000 00000000 00000000 SD:204900B0 00000000 00000000 00000000 00000000	NAND Flash CMD	SD:20480090 0000000 0000000 0000000 0000000 SD:204800A0 000000 0000000 0000000 0000000 SD:204800B0 000000 0000000 0000000 00000000			
ST:0001484C BF00 nop ST:0001484E 6820 ldr	SD:204800C0 0000000 0000000 0000000 0000000 SD:204800D0 0000000 0000000 00000000 00000000	SD:204900C0 0000000 0000000 0000000 0000000 SD:204900D0 0000000 0000000 0000000 0000000	(Parameter)	SD:204B00C0 0000000 0000000 0000000 0000000 SD:204B00D0 0000000 0000000 00000000 00000000			
ST:00014850 F4407080 orr ST:00014854 6020 str ST:00014856 BDF0 pop	SD:204800E0 00000000 00000000 00000000 00000000 00000000 SD:204800F0 00000000 00000000 00000000 SD:20480100 000000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 000000000 <t< td=""><td>SD:204900E0 00000000 00000000 00000000 00000000 SD:204900F0 00000000 00000000 00000000 00000000 00000000 SD:20490100 00000000 00000000 00000000 00000000 00000000</td><td></td><td>SD:204800E0 0000000 0000000 0000000 0000000 SD:204800F0 0000000 0000000 00000000 0000000 SD:20480100 0000000 0000000 0000000 00000000</td></t<>	SD:204900E0 00000000 00000000 00000000 00000000 SD:204900F0 00000000 00000000 00000000 00000000 00000000 SD:20490100 00000000 00000000 00000000 00000000 00000000		SD:204800E0 0000000 0000000 0000000 0000000 SD:204800F0 0000000 0000000 00000000 0000000 SD:20480100 0000000 0000000 0000000 00000000			
ST:00014858 4602 mov ST:0001485A 2000 movs	SD:20480110 00110000 000000FF 00000000 00000000	SD:20490110 00110000 000002FF 00000000 00000000 SD:20490120 0000000 00000000 00001014 00000000	SD:204A0110 00110000 000002FF 0000000 00000000 SD:204A0120 0000000 00000000 0000114 00000000 SD:204A0120 00000000 00000000 0000114 00000000	SD:204B0110 00110000 000002FF 00000000 00000000 SD:204B0120 0000000 00000000 00001014 00000000			
ST:0001485C F362100F bfi ST:00014860 F3610006 bfi ST:00014864 4770 bx	SD:20480130 000000000 00000000 00000000	SD:20490130 000000000 000000000 000000000 000000000 000000000 000000000 000000000 000000000 000000000 000000000 0000000000000000 000000000000000000000000000000000000	SD:204A0130 0000000 0000000 0000000 0000000 00001F37 SD:204A0140 0000000 0000000 00000000 00000000 0000000 SD:204A0150 00000000 00000000 00000000 00000000 00000000	5D:20480130 0000000 0000000 0000000 00001F37 5D:20480140 0000000 00008000 00000000 00000000 5D:20480150 0000000 00000000 00000000 00000000			
ST:00014866 4A5C 1dr ST:00014868 EB024000 add	SD:20480160 0000000 0000000 0000000 0000000 SD:20480170 0000000 0000000 00000000 00000000	SD:20490160 00000000 00000000 00000000 00000000 SD:20490170 00000000 00000000 00000000 00000000	SD:204A0160 0000000 00000000 00000000 00000000 SD:204A0170 0000000 00000000 00000000 00000000	SD:204B0160 0000000 0000000 0000000 0000000 SD:204B0170 0000000 0000000 00000000 00000000			
ST:0001486C 89C0 ldrh ST:0001486E 2201 movs ST:00014870 408A lsls	5D:20480180 0000000 00000000 00000000 V	SD:20490180 00000000 00000000 00000000 ✓ <	SD:204A0180 0000000 0000000 00000000 V < > .:i	<u>5D:204B0180</u> 00000000 00000000 00000000 ♥			
ST:00014872 4210 tst ST:00014874 D001 beq	B::Data.dump (0x204C0000) /NoAscii /DIALOG ロ 図 S	Will B::Data.dump (0x204D0000) /NoAscii /DIALOG ロ 回 図	; [B::Data.dump (0x204E0000) /NoAscii /SpotLig 🗖 🔲 🖾				
ST:00014876 2000 movs ST:00014878 4770 bx ST:0001487A 2001 movs	C:0x204C0000	C:0x204D0000	C:0x204E01E0 护Find Modify Long ~ □	C:0x204F0000 前Find Modify Long ~ [
ST:0001487C 4770 bx ST:0001487E 4A56 ldr	address 0 4 8 C SD:204C0000 +0000001F 00000003 00000000 00000000 ^	address 0 4 8 C SD:204D0000 +0000001F 00000001 00000000 00000000 A	address 0 4 8 C SD:204E01E0 00000000 00010000 00000000 000034B8	address 0 4 8 C SD:204F0000 +0000001F 00000003 00000000 00000000 ^			
ST:00014880 E8024000 add ST:00014884 6802 ldr ST:00014886 F3610203 bfi	SD:204C0010 0000000 0000000 0000000 0000000 SD:204C0020 0000000 0000000 00804003 0000000 SD:204C0030 0000000 00000000 00000000 00000000	SD:20400010 00000000 00000000 00000000 00000000 00000000 E SD:20400020 00000000 00000000 00000000 00000000 E E SD:20400030 00000000 00000000 00000000 00000000 E E	SD:204E01F0 0000FFFF 83F75C00 00000000 00000000 SD:204E0200 0000000 00000000 00000000 00000000	SD:204F0020 0000000 0000000 0000000 0000000 SD:204F0020 0000000 0000000 0000000 0000000 SD:204F0030 0000000 00000000 00000000 00000000			
ST:0001488A 6002 str ST:0001488C 6841 ldr	SD:204C0040 0000000 0000000 0000000 0000000 SD:204C0050 0000000 00000000 00000000 ^ ^	SD:204D0040 0000000 0000000 0000000 0000000 SD:204D0050 0000000 0000000 00000000 00000000	SD:204E0220 0000000 0000000 0000000 00000000 SD:204E0230 0000000 0000000 00000000 00000000	SD:204F0040 0000000 0000000 0000000 0000000 SD:204F0050 0000000 0000000 00000000 00000000 ^			
ST:0001488E F4413100 orr ST:00014892 6041 str ST:00014894 6941 ldr	SD:204C0060 0000000 0000000 0000000 0000000 SD:204C0070 0000000 0000000 0000000 0000000 SD:204C0080 0000000 0000000 0000000 0000000	SD:20400060 000000000 00000000 00000000	SD:204E0240 0000007 00000001 00000000 00000000 SD:204E0250 0000000 0000000 0000000 0000000 SD:204E0260 0000000 0000000 00001401 0000000	SD:204F0060 0000000 0000000 0000000 0000000 SD:204F0070 0000000 0000000 0000000 0000000 SD:204F0080 0000000 0000000 00000000 0000000			
ST:00014896 F0410101 orr ST:0001489A 6141 str	5D:204C0090 0000000 0000000 0000000 0000000 5D:204C00A0 0000000 0000000 00000000 00000000	SD:204D030 0000000 0000000 0000000 0000000 SD:204D0030 0000000 0000000 00000000 00000000 SD:204D00A0 0000000 0000000 00000000 00000000		SD:204F0090 0000000 0000000 0000000 0000000 SD:204F00A0 0000000 0000000 00000000 00000000			
ST:0001489C 6841 1dr ST:0001489E F4213100 bic ST:000148A2 6041 str	SD:204C00B0 00000000 00000000 00000000 00000000 00000000 00000000 SD:204C00C0 00000000 00000000 00000000 SD:204C00D0 00000000 00000000 00000000 SD:204C00D0 00000000 00000000 00000000 00000000 SD:204C00D0 000000000 000000000 0000	SD:20400080 0000000 0000000 0000000 0000000 SD:204000C0 0000000 0000000 0000000 0000000 SD:204000D0 00000000 00000000 00000000 00000000	NAND Flash CMD	SD:204F0080 0000000 0000000 0000000 0000000 SD:204F00C0 0000000 0000000 0000000 0000000 SD:204F00D0 0000000 0000000 00000000 0000000			
ST:000148A4 4770 bx ST:000148A6 494C ldr	SD:204C00E0 0000000 0000000 00000000 00000000 SD:204C00F0 00003366 0000024E 0000024E 4E4F5A4C	SD:204D00E0 0000000 0000000 0000000 0000000 SD:204D00F0 00003366 00000084 0000084 4E4F5A4C	(Primary)	SD:204F00E0 0000000 0000000 0000000 0000000 SD:204F00F0 000000CE 00000001 00000000 45524944			
ST:000148A8 EB014000 add ST:000148AC 68C0 1dr ST:000148AE B280 uxth	SD:204C0100 02A49F13 0000000 0000000 00003366 SD:204C0110 0001001 4154454D 00000015 0000000 SD:204C0120 0000000 0000000 00003366 0000024E	SD:204D0100 02906BC7 0000000 0000000 00003366 SD:204D0110 00010002 4154454D 00000024 00000000	SD:204E0300 0000000 00000000 00000000 00000000	SD:204F0100 0287D57E 00000000 00000000 000000CE SD:204F0110 0001001 4154454D 0000001 0000000 SD:204F0120 00000000 00000000 000000CE 00000001			
ST:000148B0 4770 bx ST:000148B2 4A49 ldr	SD:204C0130 0000024E 4E4F5A4C 02A49F13 0000000 SD:204C0140 0000000 00003366 00010001 4154454D	SD:204D0120 0000000 0000000 0000000 SD:204D0130 0000000 00000000 0000000 SD:204D0140 00000000 00000000 00000000	SD:204E0310 00000000 00000000 00000000 00000000	5D:204F0130 0000000 45524944 0287D57E 00000000 5D:204F0140 0000000 000000CE 00010001 4154454D			
ST:00014884 B289 uxth ST:00014886 EB024000 add ST:0001488A FB0C1 str	SD:204C0150 00000015 00000000 00000000 00000000 SD:204C0160 00000000 00000000 00000000 00000000 SD:204C0170 00000000 00000000 00000000 00000000	SD:204D0150 00000000 00000000 00000000 00000000 SD:204D0160 00000000 00000000 00000000 00000000	SD:204E0330 00000CE 000000F 01FFFFF 00330000 SD:204E0340 028F51A8 00000000 00000000 00000CE SD:204E0350 00010002 4154454D 00000051 00000000	SD:204F0150 0000001 0000000 0000000 0000000 SD:204F0160 0000000 0000000 0000000 0000000 SD:204F0170 0000000 0000000 00000000 0000000			
ST:0001488C 4770 bx v	5D:204C0180 00000000 00000000 00000000 00000000	5D:204D0170 0000000 00000000 00000000 00000000 5D:204D0180 0000000 00000000 00000000 00000000 v	SD:204E0360 00000000 00000000 000000423	SD:204F0180 00000000 00000000 00000000 00000000			
B::							
ST:00014846 stopped at breakpoint MIX UP dial							

NAND Flash Command in Flash Channel Buffer

Flash Interface Layer



Steps : Access All Physical Block





DEMO : Access All Physical Block



Okay, then what can we do with it?

- Non Security Encoding-SSD
 - Data Restoration

 \checkmark Unique PBA blocks not found in the LBA

• Forensics

 \checkmark Image based on LBA \rightarrow Image based on PBA

 \checkmark Non-Destructive

Okay, then what can we do with it?

- Security Encoding-SSD
 - Secure Erase Verification

 \checkmark Whether SSD still leaves sensitive data or not

Access to Factory Reserved Area

 \checkmark You may find Critical Information in SSD

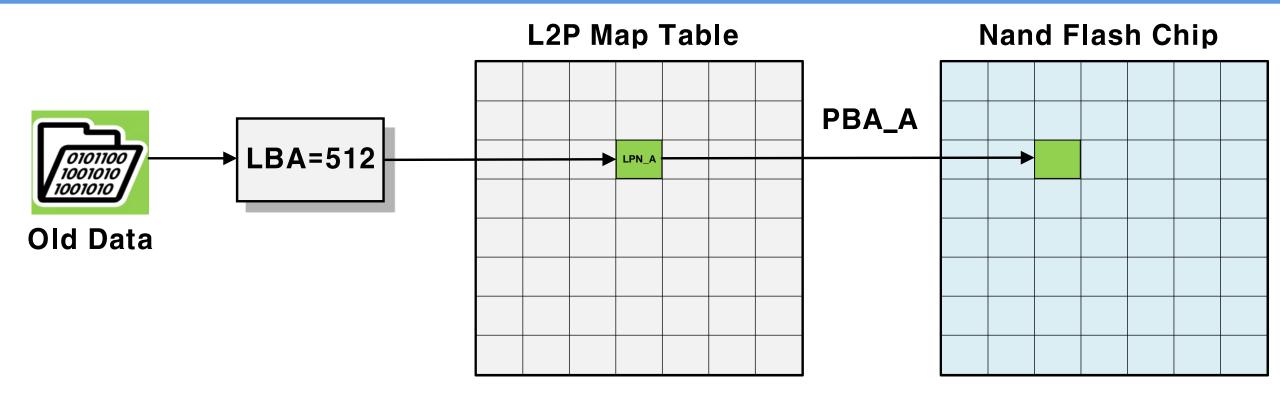
✓ Generally, Not Encrypted



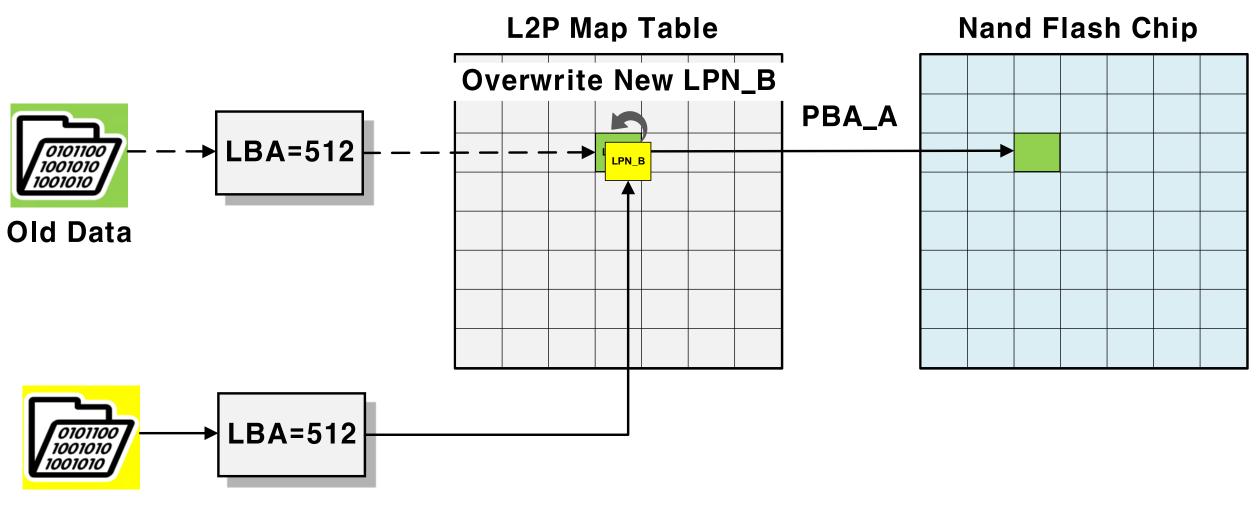
SSD Firmware Reversing

Recover Overwritten Data

Overwrite to Same LBA

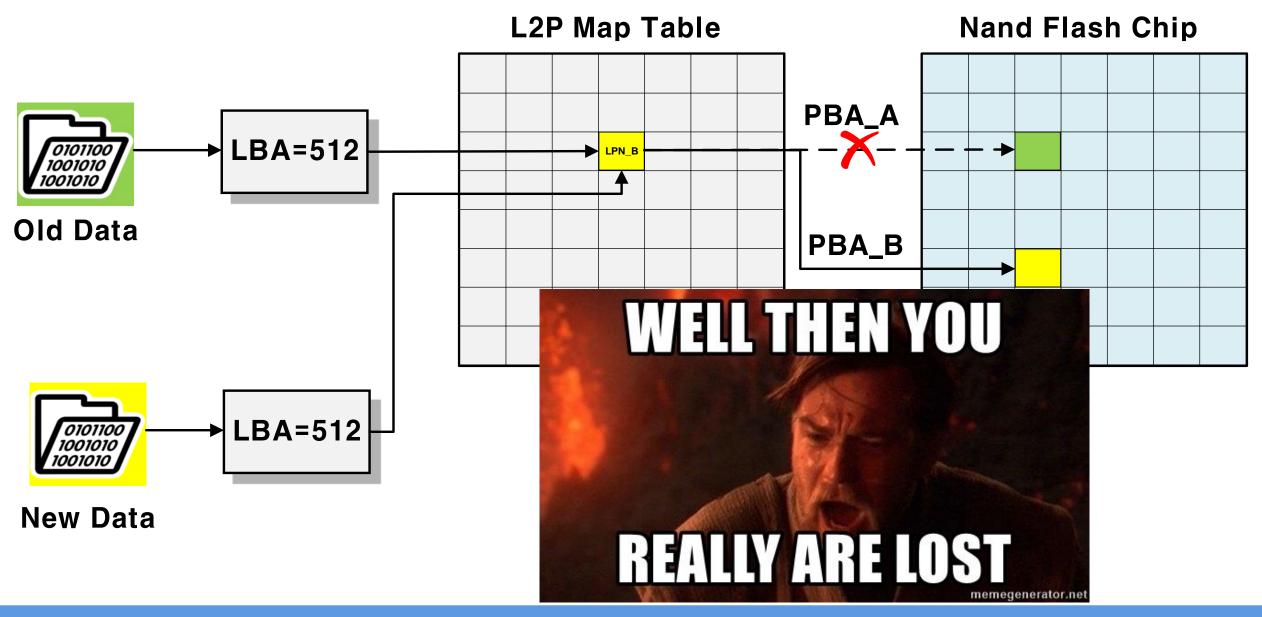


Overwrite to Same LBA

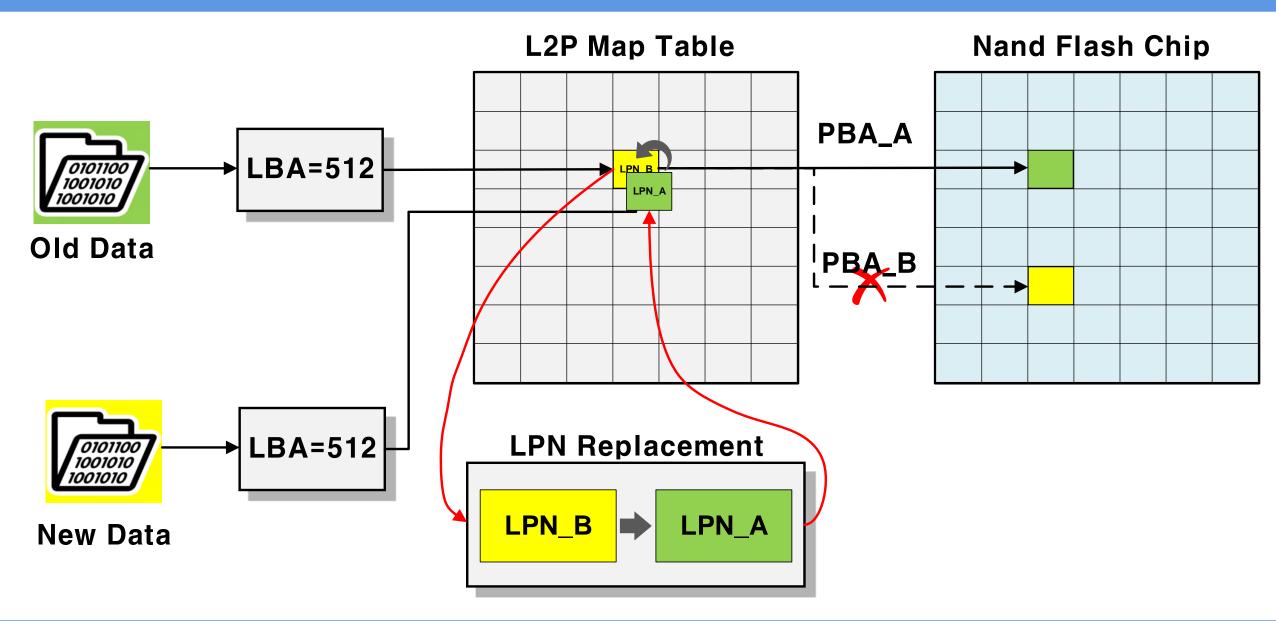


New Data

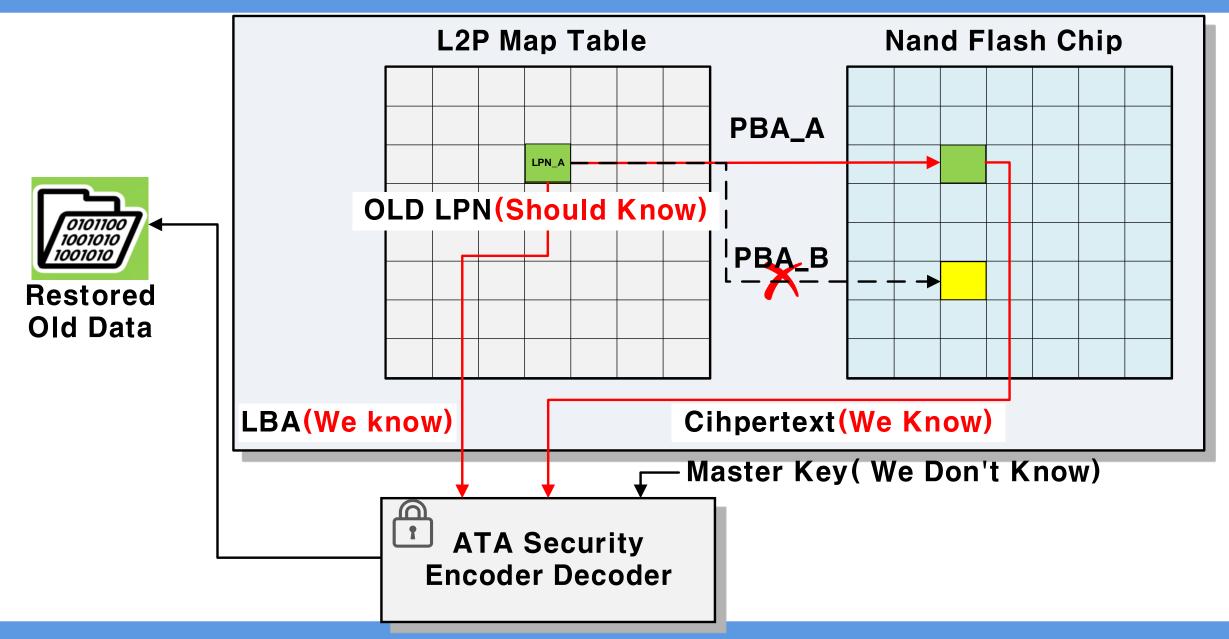
Overwrite to Same LBA



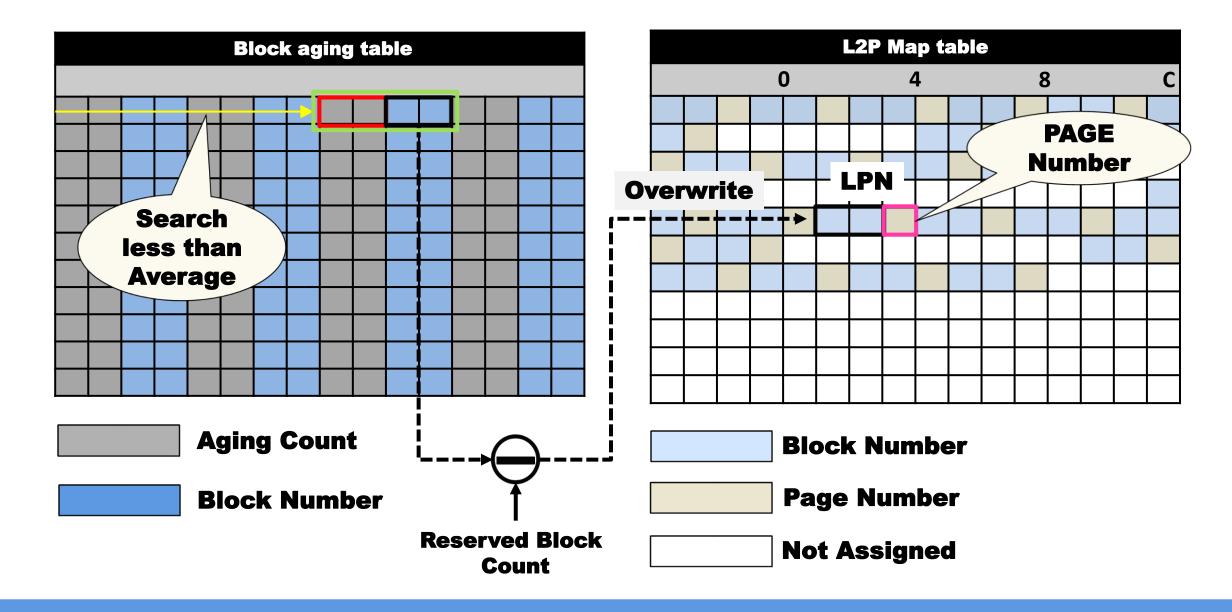
IS It Still Alive?



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



Block aging table and Data Overwriting



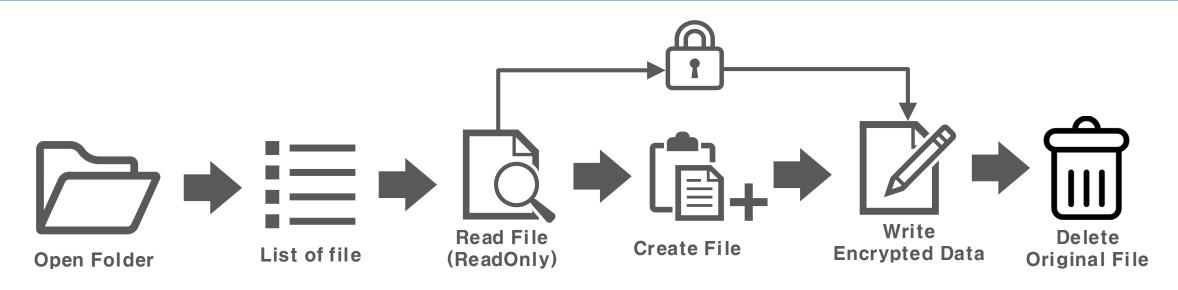
Mapping Technique and Data Overwriting

	LPN			16 bit (block)		7 bit (offse	et) 1 bit
					Block 0 Page 0	Block 1 Page 0	Block 2 Page 0
	Overwrite cnt=0	Overwrite cnt=1	Overwrite cnt=2	Overwrite cnt=3			Page 1
LBA	LPN (Block, Offset)	LPN (Block, Offset)	LPN (Block, Offset)	LPN (Block, Offset)	Page 88	Page 46	Page 2
43	(2,3)	(2,4)	(2,5)	(2,6)	Page 89	Page 47	Page 3
72	(0,88)	(0,89)	(0,90)	(0,91)	Page 90	Page 48	Page 4
84	(1,46)	(1,47)	(1,48)	(1,49)	Page 91	Page 49	Page 5
					Page max	Page max	Page max

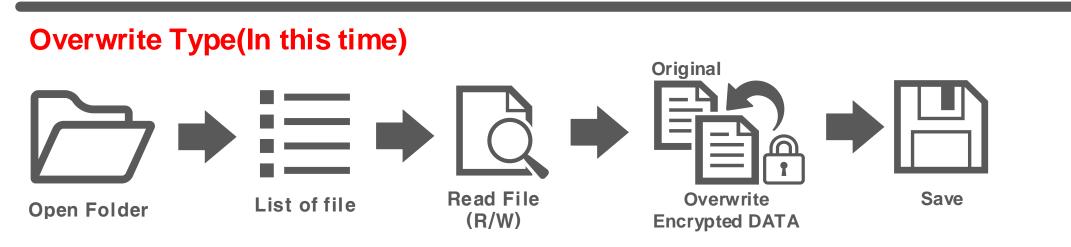
Mapping Technique and Data Overwriting



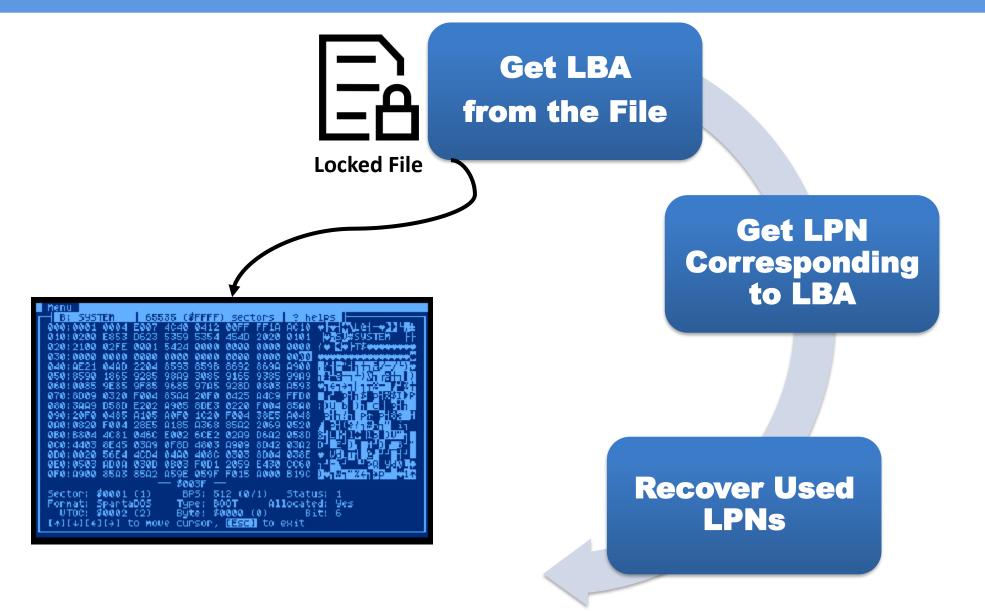
Type of Ransomware : Overwrite or Copy



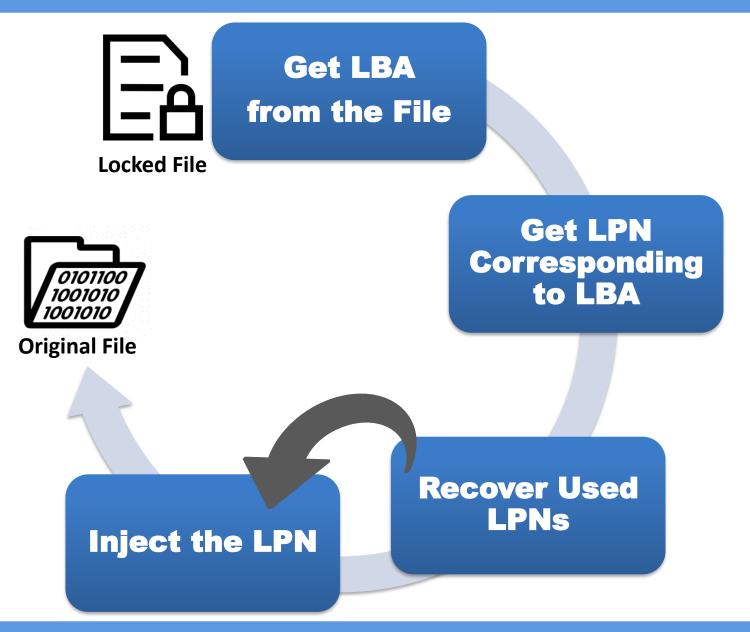
Copy And Delete Type



Steps : Overwritten Data Restoration



Steps : Overwritten Data Restoration





DEMO : Overwritten Data Restoration



- 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.

black hat EUROPE 2020

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



Youtube Channel SNTWORKS Inc.



#BHEU @BLACKHATEVENTS