

eMMC CHIPS. DATA RECOVERY BEYOND CONTROLLER Rusolut



APPLICATIONS OF EMMC CHIPS

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

...AND MUCH MORE...



DIFFERENT WAYS OF IMAGE EXTRACTION FROM DEVICES BASED ON EMMC CHIPS





CLASSIC CHIP-OFF AND DATA EXTRACTION FROM eMMC CHIP



CLEANING



PHYSICAL IMAGE EXTRACTION





FLASH MEMORY CHIPS

NAND

eMMC



..... -..... -.... **OF INTEREST** AREA -..... -----..................... •

EMMC vs RAW NAND CHIP-OFF DATA RECOVERY

NAND



eMMC/eMCP







INSIDE EMMC





EMMC CHIP STRUCTURE





WHY CARE ABOUT GETTING DATA VIA NAND FROM EMMC?

- DAMAGED EMMC CHIPS
- FACTORY RESET
- ERASED DATA RECOVERY

NAND MEMORY ADDRESSING AND R/W OPERATIONS



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

PAGE IS A SMALLEST R/W UNIT

BLOCK IS A SMALLEST ERASE UNIT

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



HOW DATA MODIFICATION PROCESS IS SUPPOSED TO WORK IN NAND MEMORY



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



HOW DATA MODIFICATION PROCESS ACTUALLY WORKS IN NAND MEMORY







TO MAKE THINGS WORSE LET'S ERASE EMMC CHIP!

LET'S TRY TO EXTRACT SOME DELETED SMS FROM THOSE "OVERWRITTEN" GARBAGE BLOCKS OF EMMC MEMORY VIA NAND INTERFACE

THERE ARE SEVERAL STEPS...

- GAIN ACCESS TO NAND MEMORY OF eMMC CHIP
- EXTRACT PHYSICAL IMAGE OF NAND CHIP
- DECODE PHYSICAL IMAGE TO READABLE FORM
- CHECK IF THERE ARE STILL BLOCKS WITH "REMNANTS" IN THE DUMP (WE EXPECT TO SEE 0x00 IN THE WHOLE DUMP)
- SCAN DUMP USING SQLITE CARVING ALGORITHM TO FIND DELETED SMS
- ANALYSE RESULTS (WE EXPECT TO FIND **NOTHING!** USER'S DATA)



TECHNOLOGICAL PADS - NAND INTERFACE







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



EMMC THROUGH XRAY





NAND PINOUT ANALYSIS. XRAY





DELAYERED EMMC CHIP





NAND PINOUT ANALYSIS. LOGIC ANALYZER





NAND PINOUT ANALYSIS. LOGIC ANALYZER

Bury Day Day <th>Acquired: 18:24:08.877</th> <th>8.41 ms 8.</th> <th>.41 ms 8.42 ms</th> <th>8.42 ms 8.42 ms</th> <th>8.42 ms</th> <th>8.4</th> <th>2 ms</th> <th>8.43 n</th> <th>ns</th> <th>8.43 ms</th> <th>8.43 ms</th> <th>8.43</th> <th>ms 8.43 m</th> <th>ns 8.44 m</th> <th>ns 8.44 ms</th> <th></th>	Acquired: 18:24:08.877	8.41 ms 8.	.41 ms 8.42 ms	8.42 ms 8.42 ms	8.42 ms	8.4	2 ms	8.43 n	ns	8.43 ms	8.43 ms	8.43	ms 8.43 m	ns 8.44 m	ns 8.44 ms	
1000 10000 1000	•		Busy													
			Dusy													
mula	I/00-0															
1 0.00000 0.0000 0.0000 0.00000 0.00000 0.00000 0.00000 0.00000 0.00000 0.00000 0.00000 0.00000 0.00000 0.00000 0.00000 0.00000 0.00000 0.00000 0.000000 0.000000 0.000000	I/01-1								Π			מתרדים ממר מינר	ית המתחה הת התחומה	ת הה ההריחה הוחורה	הרורים היה היה הרוורדים הוו	
I BUS I BUS <th< td=""><td>T/02-2</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>Ű</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></th<>	T/02-2								Ű							
1005 1005 <td< td=""><td>1/02-2</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></td<>	1/02-2															
I 00-4	I/03-3															
BUB	I/04-4															
2 BUS (MAD) 1/25-6 1/25-7<	I/05-5															
	BUS_NAND F								/\ [] []							
10000 100000 100000 10000 10000 10000 100000 100000 100000 100000 100000 100000 100000 100000 100000 100000 100000 100000 100000 100000 100000 1000000 1000000 1000000 <	1/00-0								IUI						יישה ההיהה היה היהה היהה היהה היהה היהה	
	I/07-7															
NL-10 ZP-13 Pr(0-14 NL-10 ZP-13 ZP-13 NL-10 ZP-13 NL-10 ZP-13 <td>CLE-11</td> <td></td>	CLE-11															
22-13 (72-9) 22-14 (72-14) 22-14 (72-14) </td <td>ALE-10</td> <td></td> <td>7</td> <td></td> <td></td>	ALE-10													7		
Market Market<	DF# 12						<u> </u>									
Name Order Order <tho< td=""><td>RE#-13</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tho<>	RE#-13															
Each Channel Command Row Address(h) Column / Feature Address(h) D0 D1 D2 D3 D4 D5 D6 D7 ASCII(D0-D7) Sample Command Row Address(h) Column / Feature Address(h) D0 D1 D2 D3 D4 D5 D6 D7 ASCII(D0-D7) 9 6.13124ms READ #2(30) 00000 51 62 99 93 62 F5 93 D0 Q 99 6.12124ms READ #2(30) 00000 0000 51 62 F9 AA 06 43 AB 60 F C.m 93 93 93 93 93 94 70 04 Ar 7	WE#-9															
Label Channel Sample Command Row Address(h) Column / Feature Address(h) D0 D1 D2 D3 D4 D5 D6 D7 ASC(ID-D7) 98 0.42445m8 READ 000412 0000 51 97 93 62 75 93 8D 0 ASC(ID-D7) 99 0.42245m8 READ 00060 0000 38 0.4 75 93 8D 0 101 0.63257m8 READ 2(30) 000600 0000 38 0.4 75 93 8D 0 0 102 0.53057m8 READ 2(30) 000600 0000 41 76 92 0.4 43 AB 6D 7C.m 103 9.565925m2 READ 2(30) 000601 0000 41 76 92 93 62 75 93 8D 0m 105 9.565058m2 READ 2(30) 00040A 00000 41 76 92 93 62 75	NAND Flash R/B#0-	14													₽.	,₽
Base Distant Distant <thdistant< th=""> <thdistant< th=""> <thdist< td=""><td>Label Channe</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>I</td><td><u> </u></td><td></td><td></td><td></td><td></td><td>•</td></thdist<></thdistant<></thdistant<>	Label Channe									I	<u> </u>					•
CHOO Diss Sample Command Row Address(h) Column / Feature Address(h) D0 D1 D2 D3 D4 D5 D6 D7 ASCII(00-D7) 99 9.1214ma ESET (F7) 000412 00000 51 P9 93 62 P5 93 D0 0 101 0.2352ma FEAD \$1(00) 000600 00000 38 0A F9 AA 06 43 AB 6D 7 C.m. 102 9.3050ma FEAD \$2(30) 000601 0000 00 0 <t< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></t<>																
Line Data Data <thdata< th=""> Data Data <thd< td=""><td></td><td>i j</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></thd<></thdata<>		i j														
Sample Command Row Address(h) Column / Feature Address(h) D0 D1 D2 D3 D4 D5 D6 D7 Ascli(00-D7) 98 0.34249ms READ #2(30) 00000 0000 51 87 99 93 6E F5 53 8D 0n 101 0.2527man READ #2(30) 000000 0000 38 0A F9 AA 06 43 AB 6D 7C.m 103 9.35593ms READ #2(30) 000000 0000 41 76 92 93 6E F5 A3 AB 6D 7C.m 104 9.3565325ms READ #2(30) 000601 0000 41 76 92 59 A9 70 44 Avp. 105 9.51633ms READ #1000 00040A 0000 4C C1 0A 03 D3 C4 D5 A7 L 106 9.516455ms R	CH-00 Bus BUS NA	ND Flash(NAND Flash)										Q	Search All Field			A V
Sample Command Row Addres(h) Ocolumn / Fedure Addres(h) D0 D1 D2 D3 D4 D5 D6 D7 ASCII(00-D7) 99 8.424ma REXD #1(0) 0000 0000 51 97 93 6E F5 93 0																
20 0.73429mm READ (20) 000012 0000 51 61 93 62 <	Sample	Command	Row Address(h)	Column / Feature Addres	is(h) D0	DI	D2	D3	D4	D5	D6 D7	0 -		ASCII(D0-D7)		
200 0.02570ms READ #1(00) 000600 0000 3B 0A F9 AA 06 43 AB 6D 7C.m 101 8.25570ms READ #1(00) 000601 0000 3B 0A F9 AA 06 43 AB 6D 7C.m 103 9.356925ms READ #1(00) 000601 0000 41 76 9E C9 19 A9 70 04 Avp. 104 9.356925ms READ #1(00) 00040A 0000 41 76 9E C9 19 A9 70 04 Avp. 105 9.51605ms READ #1(00) 00040A 0000 42 0 <t< td=""><td>98 8.34249ms 99 8.81214ms</td><td>READ #2(30) RESET(FE)</td><td>000412</td><td>0000</td><td>51</td><td>18</td><td>99</td><td>93</td><td>6L</td><td>15 5</td><td>13 8D</td><td>Qn</td><td></td><td></td><td></td><td></td></t<>	98 8.34249ms 99 8.81214ms	READ #2(30) RESET(FE)	000412	0000	51	18	99	93	6L	15 5	13 8D	Qn				
101 9.33052ms READ #2(30) 000600 0000 3B 0A F9 AA 06 43 AB 6D fC.m 102 9.35095ms READ #2(30) 000601 0000	100 8.82578ms	READ #1(00)	000600	0000												
102 9.35095ms READ #1(00) 000601 0000 1 7 9 6 1 <th1< td=""><td>101 8.83052ms</td><td>READ #2(30)</td><td>000600</td><td>0000</td><td>3B</td><td>0A</td><td>F9</td><td>AA</td><td>06</td><td>43 <i>I</i></td><td>.B 6D</td><td>;C.m</td><td></td><td></td><td></td><td></td></th1<>	101 8.83052ms	READ #2(30)	000600	0000	3B	0A	F9	AA	06	43 <i>I</i>	.B 6D	;C.m				
103 9.365925ms READ #1(00) 000601 0000 4 76 96 76	102 9.35098ms	RESET (FF)														
104 9.370675ms READ #2(30) 000601 0000 41 76 9E C9 19 A9 A9 A9 A7 Arp. 105 9.5153ms READ #2(30) 00040A 0000 4C C1 0A 03 D3 C4 D5 A7 L 106 9.516805ms READ #2(30) 000412 0000 6E F5 93 6E F3 F3 F7	103 9.365925ms	READ #1(00)	000601	0000												
103 9.315338 READ #1(00) 00040A 0000 400 600	104 9.370675ms	READ #2 (30)	000601	0000	41	76	9E	C9	19	A9 7	0 04	Avp.				
Note	105 9.51535ms	READ #1(00) READ #2(30)	00040A	0000	4C	C1	02	03	D3	C4 T	5 27	T				
108 9.96645ms READ #2(30) 000412 0000 51 8F 99 93 6E F5 93 8D Qn. 109 10.4473ms READ #2(30) 000413 0000 01 DF 7E 1B 07 8F 2D F7	107 9.965015ms	READ #1(00)	000412	0000	40	01	UA .	00	23	04 1	,5 A/	2				
109 10.4473ms READ #1 (00) 000413 0000 <	108 9,966495ms	READ #2(30)	000412	0000	51	8F	99	93	6E	F5 9	3 8D	0n				
110 10.448715ms READ #2 (30) 000413 0000 01 DF 7E 1B 07 8F 2D F7 111 10.92589ms RESET (FF) 000 00 </td <td>109 10.4473ms</td> <td>READ #1(00)</td> <td>000413</td> <td>0000</td> <td></td>	109 10.4473ms	READ #1(00)	000413	0000												
111 10.92589ms RESET (FF) FFF FF FFF FF </td <td>110 10.448715ms</td> <td>READ #2(30)</td> <td>000413</td> <td>0000</td> <td>01</td> <td>DF</td> <td>7E</td> <td>1B</td> <td>07</td> <td>8F 2</td> <td>D F7</td> <td></td> <td></td> <td></td> <td></td> <td></td>	110 10.448715ms	READ #2(30)	000413	0000	01	DF	7E	1B	07	8F 2	D F7					
112 10.940395ms RESET (FF) FFF FF FFF FF 00	111 10.92589ms	RESET (FF)														
113 10.94419ms RESET (FF) 114 11.04347ms RESET (FF) 115 11.05801ms RESET (FF) 115 11.05801ms RESET (FF) 115 11.05801ms RESET (FF) 115 11.0518ms	112 10.940395ms	RESET (FF)	FFFFF	FFFF												
114 11.04347ms RESET (FF) FFF FFFF FFF FF FF </td <td>113 10.94419ms</td> <td>RESET (FF)</td> <td></td> <td></td> <td>00</td> <td>00</td> <td>00</td> <td>00</td> <td>00</td> <td>00 0</td> <td>0 00</td> <td></td> <td></td> <td></td> <td></td> <td></td>	113 10.94419ms	RESET (FF)			00	00	00	00	00	00 0	0 00					
115 11.05801ms RESET (FF) FFFFF FFFF 00	114 11.04347ms	RESET (FF)														
116 11.0618mc 17 (FF) 110 11.0618mc 17 (FF)	115 11.05801ms	RESET (FF)	FFFFF	FFFF												
	116 11.0618ms	TT (FF)			00	00	00	00	00	00 0	0 00					
		I (FF)														

NAND PINOUT





CONNECT CHIP TO ADAPTER





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





ADAPTER ASSEMBLY





RAW NAND PHYSICAL IMAGE EXTRACTION



ERROR CORRECTION CODES IN FLASH MEMORY





DATA SCRAMBLERS OF FLASH CONTROLLERS





LOGICAL IMAGE RECONSTRUCTION





IMAGE AFTER DESCRAMBLING

REMEMBER WE ZEROED THIS DEVICE? WE EXPECT TO SEE 0x00 IN EVERY SECTOR/PAGE. BUT WHAT WE ACTUALLY SEE IS A BIT DIFFERENT: - AFTER 2ND ERASE CYCLE ~1% OF BLOCKS WEREN'T ERASED

ruSolu

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

🛻 🔻 Dump viewer	Visual Nand Reconstructor - H9TP32A4GDMC_NAND	– 🗆 X
Case Navigator Hex viewer Bitmap viewer		۵
Image: New View Image: New View Image: New View Image: New View Page size Page size Pixel size Pixel size Pixel size Save all Save all Save all Save selected S	8832 Image: Show structure Show position Start: V 130633 H 154 Image: Show structure Show structure Stop: V 130633 Image: H 154 Image: Show structure Stop: V 130633 Image: H 154 Image: Show structure Stop: V 130633 Image: H 154 Image: Show structure Stop: V 130633 Image: H 154 Image: Show structure Stop: V 130633 Image: H 154 Image: Show structure Stop: V 130633 Image: H 154 Image: Show structure Stop: V 130633 Image: H 154 Image: Show structure Stop: V 130633 Image: H 154 Image: Show structure Stop: V 130633 Image: H 154 Image: Show structure Stop: V 130633 Image: H 154 Image: Show structure Stop: V 130633 Image: Show structure Image: Show structure Image: Show structure Image: Show structure Image: Show	
	View settings Selection markers	
🖉 XOR 0 🗙 💐 Workspace		÷
Eyte position: 66; Row: 130117; Address: 1149193410; • • • • • • • • • • • • • • • • • • •	00 01 02 03 04 05 06 07 08 09 0A 08 00 02 02 01 00 11 00 02 02 01 00 11 00 02 02 03<	* & +
Last active selection: address 1153/506/5 selected		

SMS CARVING

THE MOST INTERESTING PART. ARE THERE REALLY ANY MESSAGES?

•∥-						Visual Nand Reconstructor - H9TP32A4GDMC_NAND	_	\times
Case	File system	n parser						 6
Check headers	Save selected	Check file system	Create unallocated data dump	Android data extractor	SQLite carver			
පි <mark>ළි</mark> Data ar	ea 1 🗙 🌞 W	Vorkspace						
🚔 Dump								
Du	mp					First sector : 0 sectors		
						Length : 8388608 sectors		
						Data anter aller		
						Data extraction x		
						Actual data Carver/Deleted data		
						Source		
						Dump		
						Dump		
						Data partition DB files		
Event le	og explorer							857
st active s	election: add	dress 11	53750675 selected	0				

RAW CARVING RESULTS

🗸 -	-					Visual Nand Reconstructor - H9TP32A4GDMC_NAND		_	×
Cas	e	SMS carver							 ۵
Exp to ex	ort ccel	Data Re transfer uns	move elected						
SMS	carve	er 🗙 🔁 Log image	e 0 🛛 🏟 Workspace						Ŧ
Gro	up by	r: None 🗡						Find repeat: Phone	< ¢
		Phone 🖓	Timestamp (UTC+0) 🏹	Status 🖓	Folder ∇	Message	7 Algorithm		
13	~	фQфф Абон		Read/Sent	Inbox	7709 снова появился в сети 08/06/2013 в 17:17, Вы можете позвонить ему. +79289900052)�t□%	Carving algorithm	41	
14	✓	Q фф Абон ф		Read/Sent	Inbox	709 снова появился в сети 08/06/2013 в 17:17, Вы можете позвонить ему. +79289900052}�t⊡%	Carving algorithm	42	
15	~	+79289037709	6/8/2013 1:17:45 PM	Read/Sent	Inbox	Абонент +79289037709 снова появился в сети 08/06/2013 в 17:17, Вы можете позвонить ему.	Carving algorithm	43	=
16	✓	+79514982624		Read/Sent	Inbox	Этот абонент пытался Вам позвонить	Carving algorithm	20	
17	~	79514982624_		Read/Sent	Inbox	от абонент пытался Вам позвонить+	Carving algorithm	21	
18	✓	+79514982624	6/8/2013 9:58:18 AM	Read/Sent	Inbox	Этот абонент пытался Вам позвонить	Carving algorithm	43	
19	~	"LiderRosto		Unread/Unsent	Inbox	Vas ozhidaet belyiy nissan N 584Podrobnaya informaciya ob usloviyah zakaza - www.rutaxi.r	Carving algorithm	19	
20	✓	LiderRostov		Unread/Unsent	Inbox	Vas ozhidaet belyiy nissan N 584Podrobnaya informaciya ob usloviyah zakaza - www.rutaxi.ru	Carving algorithm	20	
21	✓	iderRostovn		Unread/Unsent	Inbox	as ozhidaet belyiy nissan N 584Podrobnaya informaciya ob usloviyah zakaza - www.rutaxi.ru+	Carving algorithm	21	
22	✓	?X @@@ Vas o		Unread/Unsent	Inbox	nissan N 584Podrobnaya informaciya ob usloviyah zakaza - www.rutaxi.ru+79037011111L�r🛛	Carving algorithm	38	
23	✓	X && Vas oz		Unread/Unsent	Inbox	nissan N 584Podrobnaya informaciya ob usloviyah zakaza - www.rutaxi.ru+79037011111L�r🛙	Carving algorithm	39	
24	✓	X &&& Vas ozh		Unread/Unsent	Inbox	issan N 584Podrobnaya informaciya ob usloviyah zakaza - www.rutaxi.ru+79037011111L�r□	Carving algorithm	40	
25	✓	♦♦ ♦Vas ozhi		Unread/Unsent	Inbox	ssan N 584Podrobnaya informaciya ob usloviyah zakaza - www.rutaxi.ru+79037011111L�r□	Carving algorithm	41	
26	✓	��Vas ozhid		Unread/Unsent	Inbox	san N 584Podrobnaya informaciya ob usloviyah zakaza - www.rutaxi.ru+79037011111L�r□	Carving algorithm	42	
27	✓	LiderRostov	6/7/2013 8:35:20 PM	Unread/Unsent	Inbox	Vas ozhidaet belyiy nissan N 584Podrobnaya informaciya ob usloviyah zakaza - www.rutaxi.ru	Carving algorithm	43	
28	✓	Tele2		Read/Sent	Inbox	BHECEHA CYMMA 92.50 p.	Carving algorithm	20	
29	✓	ele2/		Read/Sent	Inbox	HECEHA CYMMA 92.50 p. +	Carving algorithm	21	
30	✓	X @ BHE		Read/Sent	Inbox	50 p. +79043490004 ⊕(⊕ q	Carving algorithm	37	
31	✓	BHEC		Read/Sent	Inbox	0 p. +79043490004�(�q	Carving algorithm	38	
32	✓	BHECE		Read/Sent	Inbox	p. +79043490004 ♦(♦ q□	Carving algorithm	39	-
Posi	tion 1	1 from 205							
Р° Е	vent I	log explorer							
Last a	ctive	selection: address	0 select	ed 0					

CLEANED UP RESULTS

Visual Nand Reconstructor - H9TP32A4GDMC_NAND — Messages	с X
Export Save Find Rext	
Data extraction (Log image 0) 🚽 🗸 🛛 Messages summary 🗙 SMS carver 🛛 😤 Log image 0 👘 Workspace	÷
Messages (12) Group by: None	
	urce 🗸
1 SMS Inbox 6/8/2013 1:17:45 PM +79289037709 Абонент +79289037709 снова появился в сети 08/06/2013 в 17:17, Вы Са	arver
2 SMS Inbox 6/8/2013 9:58:18 AM +79514982624 Этот абонент пытался Вам позвонить Са	arver
3 SMS Inbox 6/7/2013 8:35:20 PM LiderRostov Vas ozhidaet belyiy nissan N 584Podrobnaya informaciya ob usloviyah Ca	arver
4 🗹 💥 SMS Inbox 6/7/2013 8:22:38 PM Tele2 BHECEHA CYMMA 92.50 p. Ca	arver
5 SMS Inbox 6/7/2013 8:53:00 AM RED TAXI Скидка 10% в Ред Такси по вашему персональному коду 1812 т. Са	arver
6 🗹 💥 SMS Inbox 6/8/2013 4:34:41 PM +79514982624 Этот абонент пытался Вам позвонить Са	arver
7 🗹 🗮 SMS Inbox 7/3/2013 6:31:25 РМ +79514982624 пожалуйста не уходи все будет подругому Са	arver
8 🗹 💥 SMS Inbox 7/1/2013 6:06:57 АМ +79514982624 Люблю заю очень!!!)) Са	arver
9 💽 💥 SMS Inbox 6/29/2013 11:10:07 AM ЕGO СЕЗОН СКИДОК ОТКРЫТ: ПРИ ПОКУПКЕ ОДНОЙ ВЕЩИ-20%, ДВУХ- Са	arver
10 SMS Inbox 6/29/2013 9:22:46 AM Tele2 29.06.2013 02:03 MCK: Y BAC HA HOMEPE +79525709690 OCTATOK MEHEE 5p. KAK PA3rOBAPuBATb nPu "0" HA C4ETE - Y3HAuTE HA Ca *111#	irver
11 🗹 💥 SMS Inbox 7/3/2013 6:31:49 РМ +79514982624 Я клянусьмамой Са	arver
12 🗹 💥 SMS Inbox 7/3/2013 7:46:26 PM +79514982624 ты меня больше не увидешьпо крайнец мере живымя знал что Са	arver
Position 1 from 12	
Event log explorer	
ast active selection: address selected selected	

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

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



SMS RECOVERY FROM 10 SMARTPHONES (SAME MODEL)

Green blocks (A,C,D,F,H,J) – more SMS were found in NAND memory chip.

Red blocks (B,E,G,I) – less SMS were found in NAND memory chip due to uncorrectable bit errors caused by threshold voltage shifts (eMMC controller handles it) during read operation

А		
Source	SMS count	Comparison
NAND	116	283%
eMMC	41	100%

F		
Source	SMS count	Comparison
NAND	47	247%
eMMC	19	100%

В		
Source	SMS count	Comparison
NAND	2377	99,75%
eMMC	2383	100%

G		
Source	SMS count	Comparison
NAND	96	74%
eMMC	129	100%

С		
Source	SMS count	Comparison
NAND	4866	103%
eMMC	4723	100%

Н		
Source	SMS count	Comparison
NAND	105	525%
eMMC	20	100%

D		
Source	SMS count	Comparison
NAND	118	144%
eMMC	82	100%

E		
Source	SMS count	Comparison
NAND	6753	71%
eMMC	9464	100%

Source	SMS count	Comparison
NAND	244	94%
eMMC	260	100%

J		
Source	SMS count	Comparison
NAND	1540	131%
eMMC	1174	100%



APPLICATIONS OF TECHNOLOGY

- DATA RECOVERY FROM DAMAGED EMMC CHIPS
- RETRIEVAL OF DELETED TEXT MESSAGES, CHATS, ETC. THROUGH NAND PROTOCOL INCLUDING GARBAGE BLOCKS ON DEEPER LEVEL THAT IS NOT ACCESSIBLE FOR CLASSIC MOBILE FORENSIC TOOLS
- DATA RECOVERY AFTER FACTORY RESET OR OTHER OPERATIONS THAT ERASE DATA

Related links:

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

https://belkasoft.com/ssd-2016-part2





THANK YOU

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

