

Komprimierte Version

Deep Flash Forensik

Tauchen, umwandeln, auswerten

ACATO GmbH

Christian Bartsch

(CFE, SV f. ITF, MCT, MCSE+I)

ACATO GmbH

Hauptsitz in München (neben KPMG und WKG)

Service Portfolio:

- IT Forensik (Handy, PC & Fraud Investigations)
- Entwicklung eigener F-Tech Lösungen
 - Software für Renditeberechnung bei Beteiligungen
 - Software für Fall Management
 - Name Profiling Software
 - Crypt Cleaner Software
- Präventionsberatung
- Datenrettung (mit eigenem Class 100 Reinraum)
- Distribution von forensischer Ausrüstung

Rahmensituation

- Ohne Chip-off ist ein Auslesen kaum noch möglich
- Sicherheitsblockaden verhindern JTAG Methoden
- BGA und eMMC Chips werden zum Problem:
 - Komplexe Signal- und Versorgungswege (Pinout => Verkabelung im 0.05mm Bereich)
 - empfindlicher (Gefahr der Beschädigung im Entnahmeprozess)
 - Anfälligkeit für teilweiser/vollständiger Totalausfall

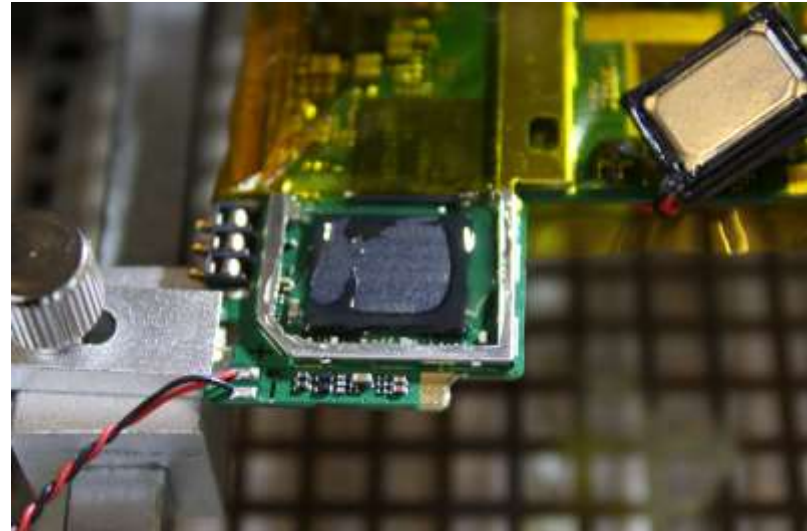


Acer z520 mit eMMC/MCP -> DRAM + Flash mit 221 BGA Aufbau

Was befindet sich im Speicher?

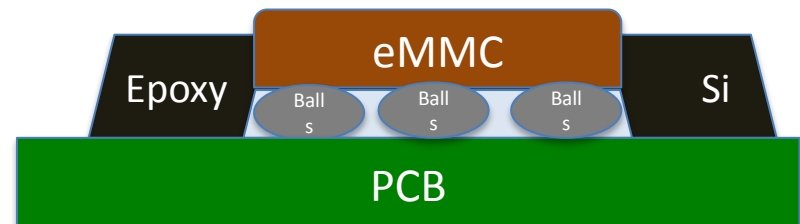
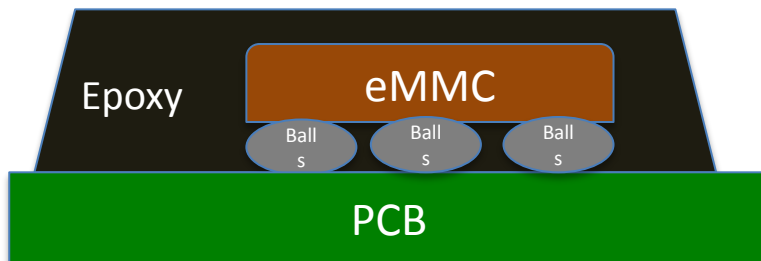
- Datenbereiche
- ECC oder BCH Codes
- XOR Keys
- Service Area
 - LBN, LPN,
 - Header,
 - Block Number
 - Plane Number
- Steuerungsdaten
- Ungenutzte Bereiche
- Sonstiges

S5 mini



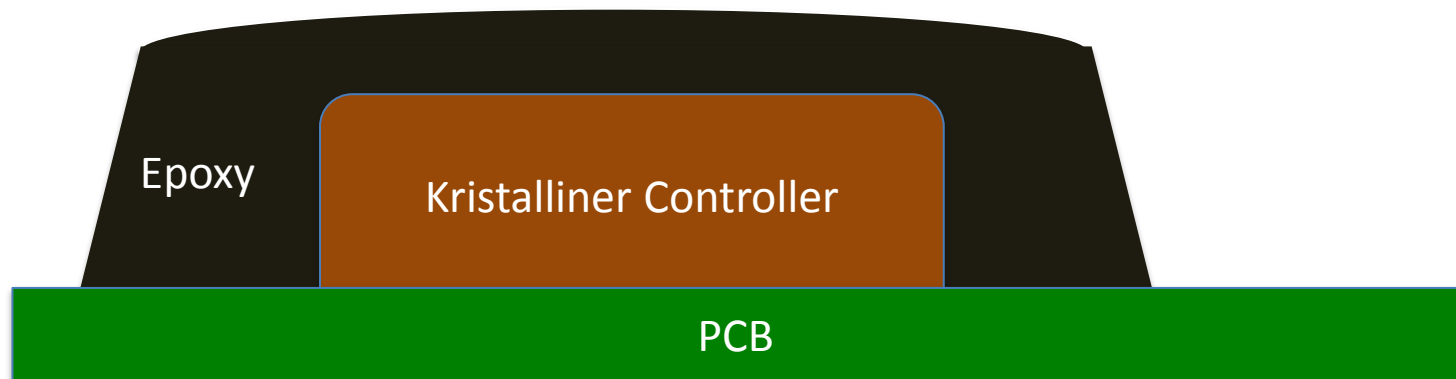
Welche Speichertypen dominieren?

- TSOP-48 bald nicht mehr dominieren außer in billigen Geräten
- BGA ohne integriertem Controller in Mid-Range Bereich
- eMMC wird in den nächsten Jahren in fast allen Geräten vorkommen!
- MCPs sind im kommen (stromsparende Kombi aus DRAM und Flash Speicher)
- eMMC und BGA Chips immer häufiger mit Epoxy vor Rissen geschützt
- eMMC mit Silikon umrahmt als weniger komplexer Schutz



Probleme im Chipoff

- Überhitzung beim Ausbau
- Fehlender Support durch gängige Systeme
- Fehlende Informationen über den Pin-Layout
- Nicht lesbare Controller Kennzeichnung
- Integrierte Controller (eventuell auch defekt)



Herausforderungen

Die Chip-off Forensik erfordert zunehmend...

- Unbekannte Strukturen zu rekonstruieren
- Schäden im Chip zu überwinden
- Schneller auf dem aktuellsten Stand zu sein
- Mehr Flexibilität in der eigenen Arbeit

Was brauchen wir für diese Aufgabe

- Chipreader
- Visual Nand Reconstruction Software
- Rework Station mit Dark Infrared
- PC gesteuerte Lötstation
- Mikroskop mit x40+ Zoom
- Analysetool für Handy Daten

Ausbau und Lösen der Chips

- Verwendung von IR bei BGA Chips
- Auslöten von TSOP48 mit SpeziallötKolben
- Epoxy BGA Chips bei spezieller Temperatur auslösen

Auch der Ausbau aus dem Gerät sollte möglichst schmerzfrei für die Platine erfolgen.

Rework erfolgt anhand von internen Temperaturtabellen

Wege zum Auslesen

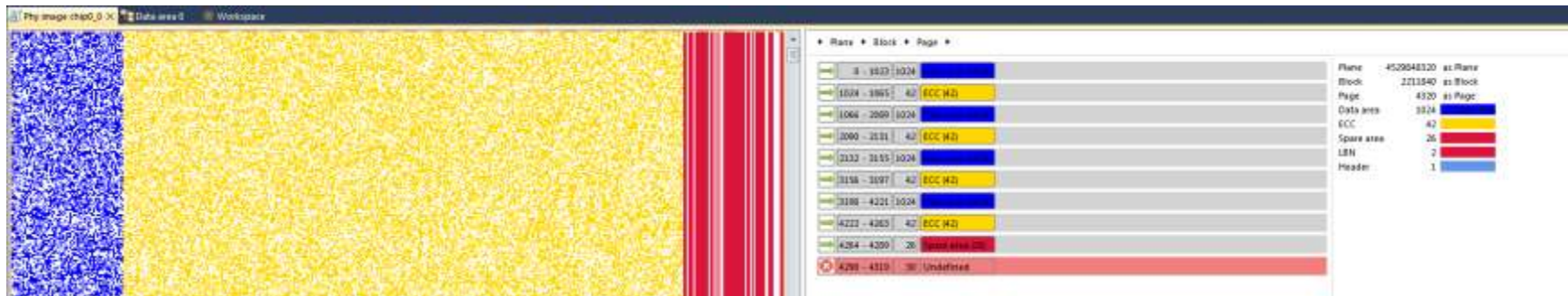
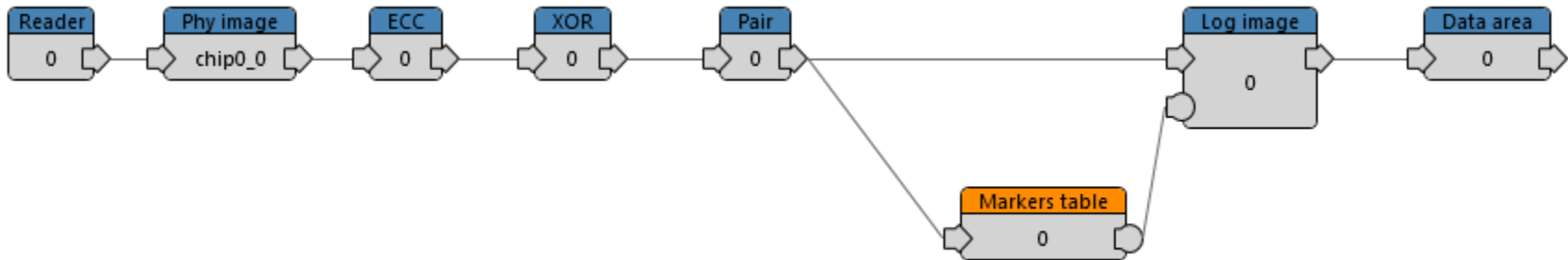
Adapter vs. Feinlöten

- Es gibt nur wenige Adapter für diverse BGA Typen
- Hohe Abnutzungserscheinungen bei Adaptern
- Adapter schon nach 5 Einsätzen beschädigt
- Preis – und Qualitätsunterschiede der Adapter

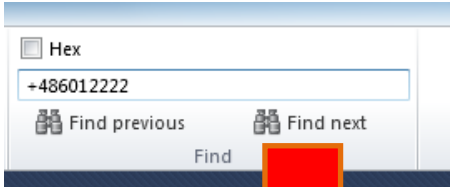
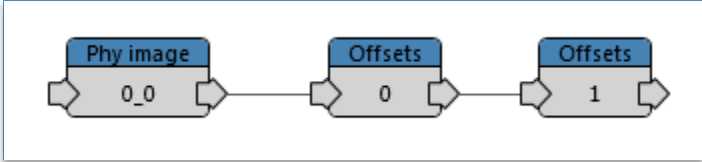
Manufaktur wird weiterhin überwiegen



Wie sieht die Arbeit aus?



Beispiel – Sony Ericsson mit BGA137



	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
0008FEF1F0	3D	2B	34	38	36	30	31	32	32	32	32	32	32	0A	09	23	=+4860122222..#
0008FEF200	23	23	23	23	23	23	23	23	23	23	23	23	23	23	23	23	#####
0008FEF210	23	23	23	23	23	23	23	23	23	23	23	23	23	23	23	23	#####
0008FEF220	23	23	23	23	23	23	23	23	23	23	23	23	23	23	23	23	#####
0008FEF230	23	23	23	23	23	23	23	23	23	23	23	23	23	23	23	23	#####
0008FEF240	23	23	23	23	23	23	23	23	0A	09	09	09	0A	FF	FF	FF	#####...YYY
0008FEF250	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	YYYYYYYYYYYYYYYY
0008FEF260	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	YYYYYYYYYYYYYYYY
0008																	YYYYYYYY

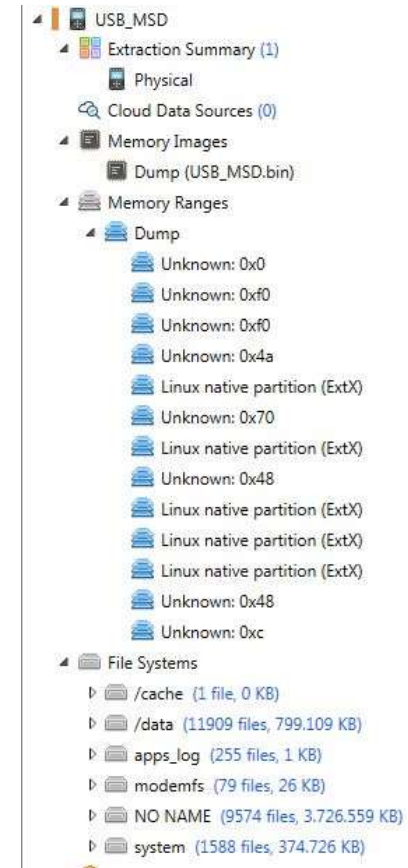
Byte position: 220; Row: 71657; Address: 151339804; Value: 11

Samsung Smartphones

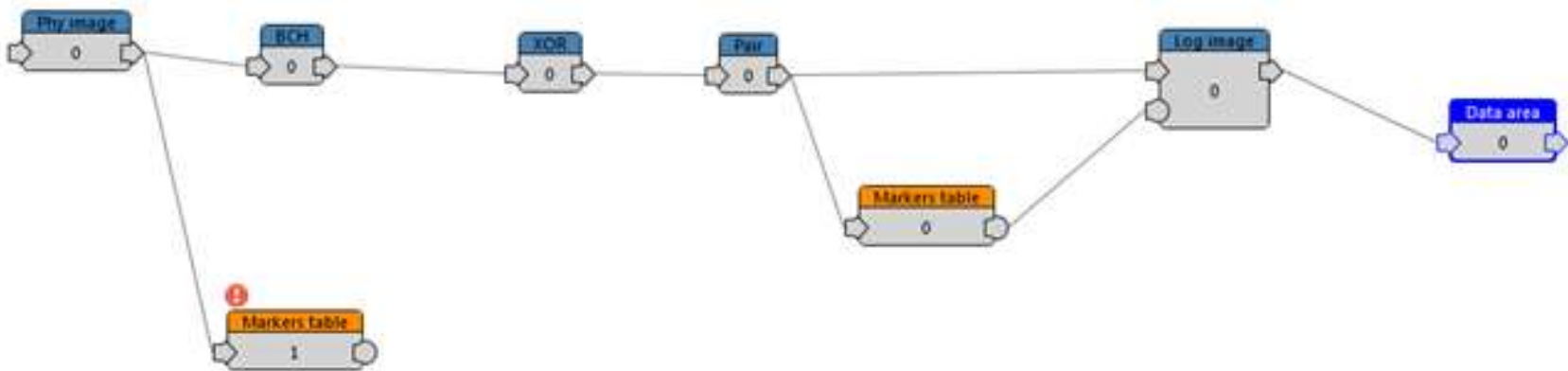
Chipoff ist bei nicht eingeschalteter
Verschlüsselung möglich!

z.B.

S4, S Duo, S5, ...



Von der Analyse zum Ergebnis



Analyse des Dumps



► Plane ► Block ► Page ►			
→	0 - 1023	1024	Data0 (1024)
→	1024 - 1031	8	SA0 (8)
→	1032 - 1073	42	ECC42 (42)
→	1074 - 2097	1024	Data0 (1024)
→	2098 - 2101	4	SA4 (4)
→	2102 - 2143	42	ECC42 (42)
→	2144 - 3167	1024	Data0 (1024)
→	3168 - 3171	4	SA4 (4)
→	3172 - 3213	42	ECC42 (42)
→	3214 - 4237	1024	Data0 (1024)

Plane	4529848320	as Plane
Block	2211840	as Block
Page	8640	as Page
Data0	1024	as Data area
ECC1	46	
ECC42	42	
SA0	8	
SA4	4	
LBN	2	
Header	1	

BCH Code finden oder recherchieren

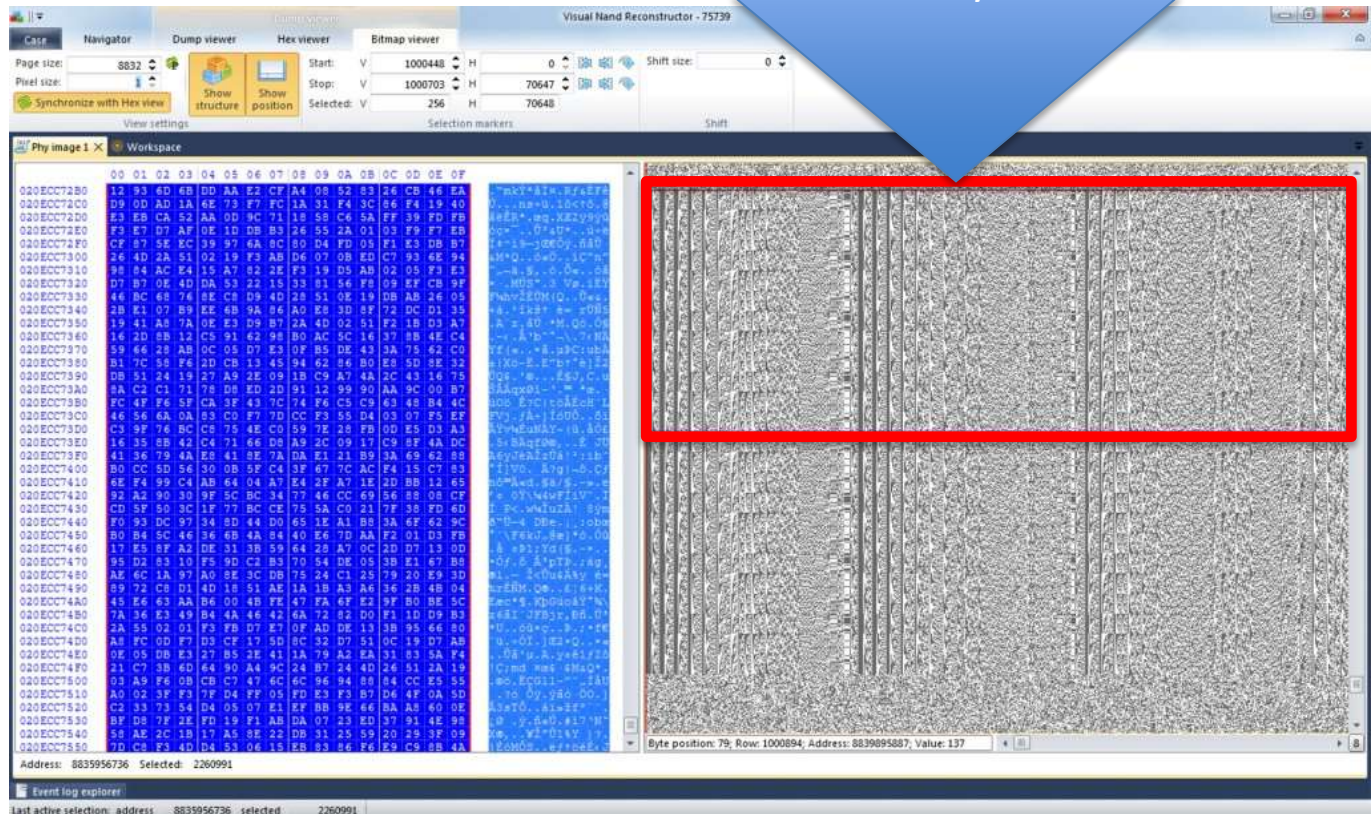
Find BCH codewords

Controller	Result	File
PS2251-50-F	15	C:\Program Files\VNR\DataBase\BCHCodewords\BCHCodewords-old\Phison\PS2251-50-F_4284_4.bch
PS2251-50-F	15	C:\Program Files\VNR\DataBase\BCHCodewords\BCHCodewords-old\Phison\PS2251-50-F_8576_8.bch
PS2251-50-F	15	C:\Program Files\VNR\DataBase\BCHCodewords\Phison\PS2251-50-F_4284_4.bch
PS2251-50-F	15	C:\Program Files\VNR\DataBase\BCHCodewords\Phison\PS2251-50-F_8576_8.bch
MS1	8	C:\Program Files\VNR\DataBase\BCHCodewords\MS1_516_1.bch
MS1	8	C:\Program Files\VNR\DataBase\BCHCodewords\BCHCodewords-old\MS1_516_1.bch
20-82	7	C:\Program Files\VNR\DataBase\BCHCodewords\BCHCodewords-old\Sandisk\Sandisk-20-82_8568(ecc78)_4.bch
20-82	7	C:\Program Files\VNR\DataBase\BCHCodewords\Sandisk\Sandisk-20-82_8568(ecc78)_4.bch
88SS8014-BHP2	7	C:\Program Files\VNR\DataBase\BCHCodewords\BCHCodewords-old\Marvell\88SS8014-BHP2_4311_2.bch
88SS8014-BHP2	7	C:\Program Files\VNR\DataBase\BCHCodewords\Marvell\88SS8014-BHP2_4311_2.bch
88SS9174-BKK2	7	C:\Program Files\VNR\DataBase\BCHCodewords\BCHCodewords-old\Marvell\88SS9174-BKK2_8590_4.bch
88SS9174-BKK2	7	C:\Program Files\VNR\DataBase\BCHCodewords\Marvell\88SS9174-BKK2_8590_4.bch
88SS9174-BLD2	7	C:\Program Files\VNR\DataBase\BCHCodewords\BCHCodewords-old\Marvell\88SS9174-BLD2_4301_2.bch
88SS9174-BLD2	7	C:\Program Files\VNR\DataBase\BCHCodewords\Marvell\88SS9174-BLD2_4301_2.bch
AU6987	7	C:\Program Files\VNR\DataBase\BCHCodewords\Alcormicro\AU6987_8576(ecc42b)_8.bch
AI16087	7	C:\Program Files\VNR\DataBase\BCHCodewords\Alcormicro\AI16087_8624_8.bch

Select Cancel

XOR Key anwenden oder erarbeiten

XOR
Key



Pair – Raid 0 Daten zusammenführen



Parameters

Enter filter string ✎

▾ **Element**

Name

▾ **Dump**

Length (bytes)

Automatic str...

▾ **Pair dump**

Number of pa... 2 ▾

Moveable blo... 8640 ▾

Area size 2211840 ▾

Markers Table

Header sowie LBN finden und kennzeichnen

The screenshot shows a forensic tool interface with a 'Markers Table' on the left and a data visualization on the right. The table lists various markers with their addresses and descriptions. The data visualization shows a grid of data points with colored vertical bars corresponding to the markers in the table.

Marker	Address	Description
Header (1)	4529848320	as Plane
Undefined	2211840	as Block
LBN (2)	8640	as Page
Undefined	1024	as Data area
ECC1	46	
ECC42	42	
SA0	8	
SA4	4	
LBN	2	
Header	1	

Logical Image

```

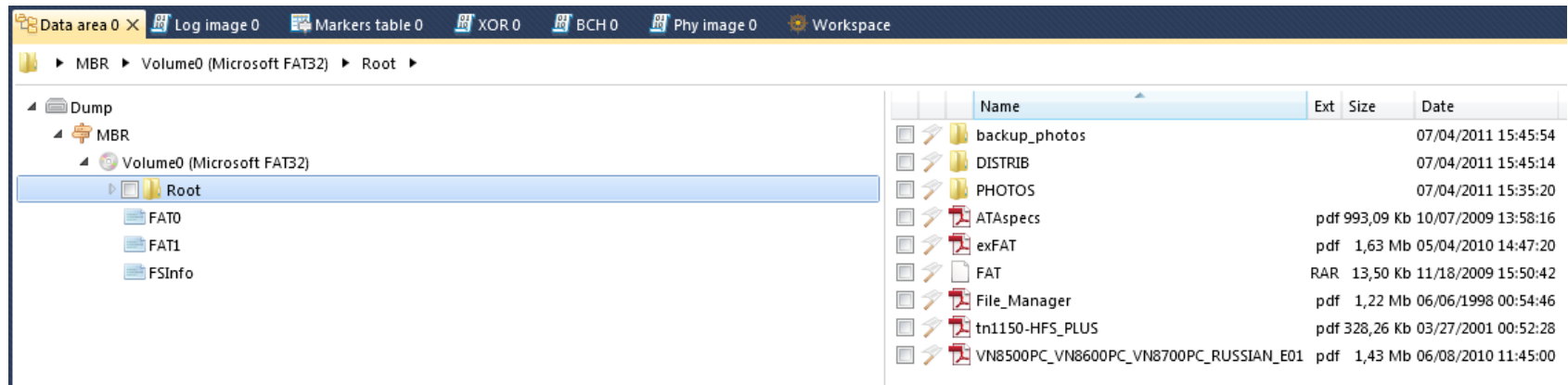
Log image 0 X Markers table 0 XOR 0 BCH 0 Phy image 0 Workspace
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
0000000000 83 C0 8E D0 BC 00 7C FB 50 07 50 1F FC BE 1B 7C 3AžĐ%.|úP.P.ú%.|
0000000010 BF 1B 06 50 57 B9 E5 01 F3 A4 CB BD BE 07 B1 04 ž...PW'á.óxÈ%%.±.
0000000020 38 6E 00 7C 09 75 13 83 C5 10 E2 F4 CD 18 8B F5 8n.|.u.f.Ā.âóí.<ó
0000000030 83 C6 10 49 74 19 38 2C 74 F6 A0 B5 07 B4 07 8B fĒ.It.8,tó u.'.<
0000000040 F0 AC 3C 00 74 FC BB 07 00 B4 0E CD 10 EB F2 88 ó-<tú»...'.í.èó^
0000000050 4E 10 E8 46 00 73 2A FE 46 10 80 7E 04 0B 74 0B N.èF.s*þF.ē~.t.
0000000060 80 7E 04 0C 74 05 A0 B6 07 75 D2 80 46 02 06 83 ē~.t. ħ.uóēF..f
0000000070 46 08 06 83 56 0A 00 E8 21 00 73 05 A0 B6 07 EB F..fV..è!.s. ħ.ē
0000000080 BC 81 3E FE 7D 55 AA 74 0B 80 7E 10 00 74 C8 A0 % >þjU*t.ē~.t.Ē
0000000090 B7 07 EB A9 8B FC 1E 57 8B F5 CB BF 05 00 8A 56 -.ēē<ü.W<óEž..šV
00000000A0 00 B4 08 CD 13 72 23 8A C1 24 3F 98 8A DE 8A FC .'.í.r#šĀq?~šBšü
00000000B0 43 F7 E3 8B D1 86 D6 B1 06 D2 EE 42 F7 E2 39 56 C+ā<Ń+Ō±.ŌiB+ā9V
00000000C0 0A 77 23 72 05 39 46 08 73 1C B8 01 02 BB 00 7C .w#r.9F.s...>|.
00000000D0 8B 4E 02 8B 56 00 CD 13 73 51 4F 74 4E 32 E4 8A <N.<V.í.sQŌtN2āš
00000000E0 56 00 CD 13 EB E4 8A 56 00 60 BB AA 55 B4 41 CD V.í.ēāšV.'>»U'Āí
00000000F0 13 72 36 81 FB 55 AA 75 30 F6 C1 01 74 2B 61 60 .r6 ūU*uošĀ.t+a`
0000000100 6A 00 6A 00 FF 76 0A FF 76 08 6A 00 68 00 7C 6A j.j.ŷm.ŷt.ĭ.h.lj
0000000110 01 6A 10 B4 42 8B F4 CD 13 61 61 73 0E 4F 74 0B .'.B<óI.aas.
0000000120 32 E4 8A 56 00 CD 13 EB D6 61 F9 C3 49 6E 76 61 2āšV.í.ēŌauĀInva
0000000130 6C 69 64 20 70 61 72 74 69 74 69 6F 6E 20 74 6E lid partition ta
0000000140 62 6C 65 00 45 72 72 6F 72 20 6C 6F 61 64 69 6E ble.Error loadin
0000000150 67 20 6F 70 65 72 61 74 69 6E 67 20 73 79 73 74 g operating syst
0000000160 65 6D 00 4D 69 73 73 69 6E 67 20 6F 70 65 72 6E em.Missing opera
0000000170 74 69 6E 67 20 73 79 73 74 65 6D 00 00 00 00 00 ting system.....
0000000180 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0000000190 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000001A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000001B0 00 00 00 00 00 2C 44 63 18 2E 07 C3 00 00 00 00 .....Dc...Ā.....
00000001C0 01 01 0C 16 D7 CA 80 1F 00 00 80 60 77 00 00 00 ....xĒē...ē`w...
00000001D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000001E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000001F0 00 00 00 00 00 00 00 00 00 00 00 00 00 55 AA .....U
0000000200 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0000000210 33 2E 32 30 2E 30 44 20 30 37 20 32 30 31 32 2 3.20.ŌD 07 2012-
0000000220 31 32 2D 33 31 00 00 00 00 00 00 00 00 00 00 00 12-31.....
0000000230 31 32 2F 30 37 2F 31 30 00 00 00 00 00 00 00 00 12/07/10.....
0000000240 31 31 3A 33 36 3A 31 33 00 00 00 00 00 00 00 00 11:36:13.....
0000000250 31 2E 31 2E 32 35 2E 30 00 00 00 00 00 00 00 00 1.1.25.0.....

```

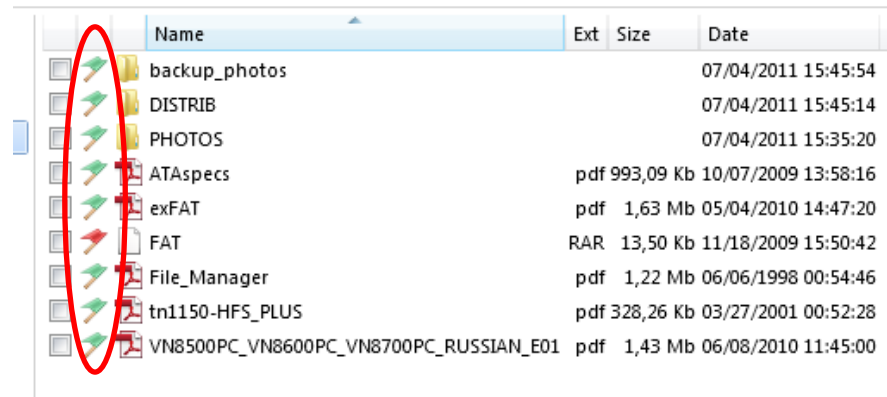
Daten werden auch in Hex lesbar
und
sind nicht mehr zerstückelt

Dump Folder Structure

- Am Ende können Dateien und Verzeichnisse sichtbar gemacht werden.



- Auch eine Header Prüfung ist möglich



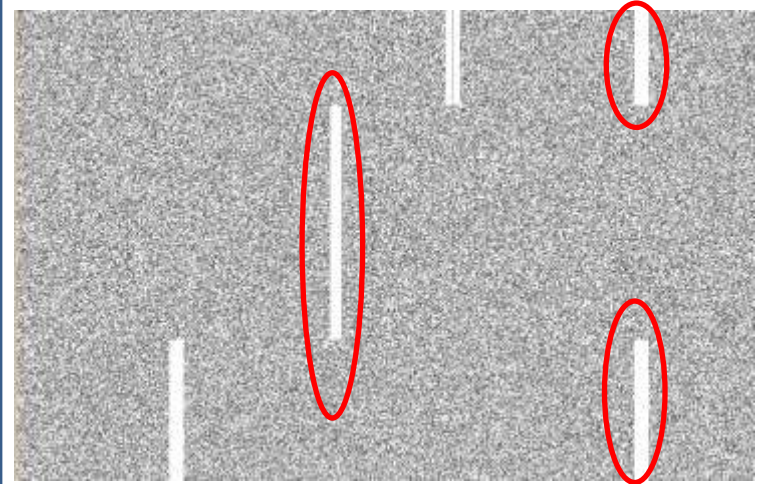
Problemlösungen

- Strom und/oder Geschwindigkeit senken
- Fehlerhafte Bereiche kennzeichnen und ausfiltern
- Serielle oder Parallele Datenbereiche sortieren
- Uvm.

Bit Errors (sehen aus wie schlechte Pixel)



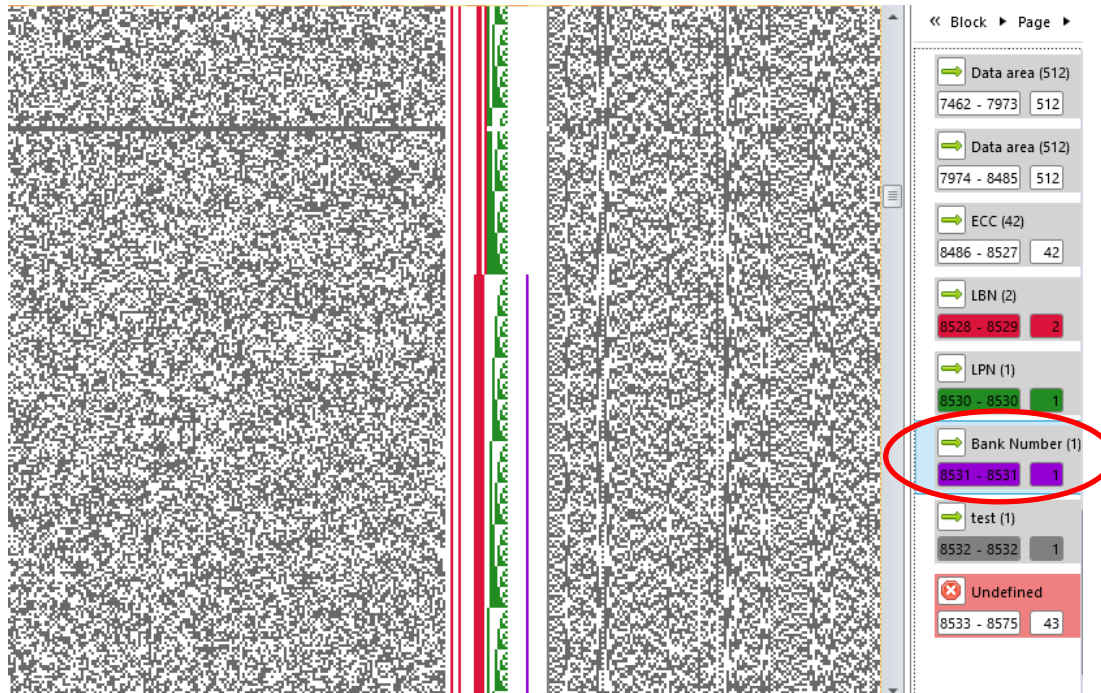
Bad Columns (Herstelldefekte)



Bank Number

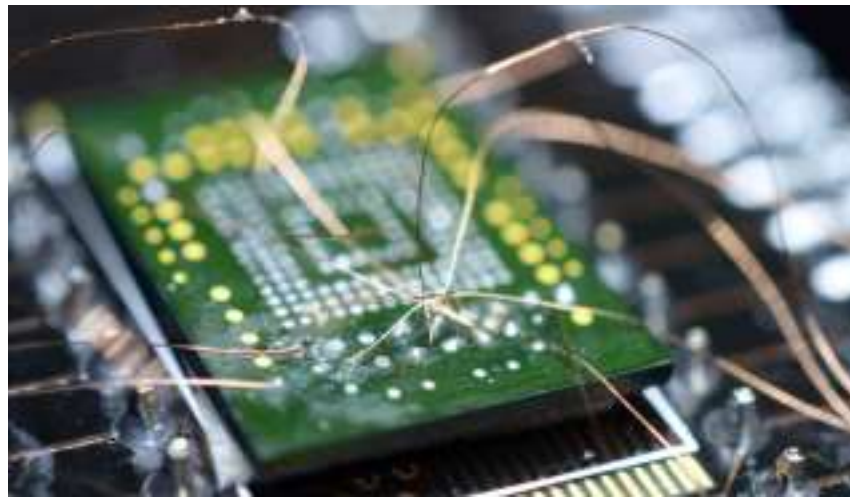
90% der Controller **verwenden keine Bank Nummer.**

Die anderen 10% der Controller lassen sich auch mit VNR lösen:



Damit können Block Filtering und Translation Tabellen aufgebaut werden

Aufwendige Verkabelungen



Interpretation von Chip Dumps

Dumps muss man analysieren und umwandeln für weitere forensische Auswertung.



Dennoch gibt es stets Risiken und Anomalien.



Was kann man untersuchen?

- Mobiltelefone (TSOP, BGA-224)
- Smartphones (BGA-136/137, BGA-169eMMC [5 Größen], MCP169/221)
- Speicherkarten (TSOP48, BGA52/100/132/152/154, Monolithic)
- USB Sticks (TSOP48, BGA, Monolithic)
- SSD Festplatten (TSOP-48/56, iNAND, eMMC)
- Geräte mit integriertem Flashspeicher (Diktiergeräte, Kameras...)
- Digitale Fahrtenschreiber
- Flugschreiber mit SLC Chips
- Sonstiges

Vielen Dank

Christian Bartsch
Geschäftsführer



ACATO GmbH
Heimeranstraße 37
80339 München

Tel. 089 / 540 41 07 - 0

www.acato.de