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 WKGT)

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

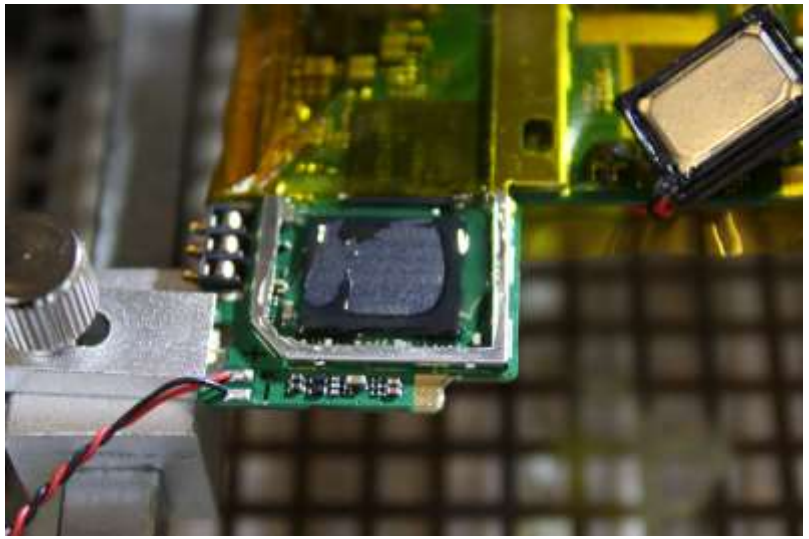
- Ohne Chip-off ist ein Auslesen kaum noch möglich
- Sicherheitsblockaden verhindern JTAG Methoden
- BGA und eMMC Chips werden zum Problem:
  - Komplexe Signal- und Versorgungswege (Pinout => Verkabelung im 0.05mm Bereich)
  - empfindlicher (Gefahr der Beschädigung im Entnahmeprozess)
  - Anfälligkeit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

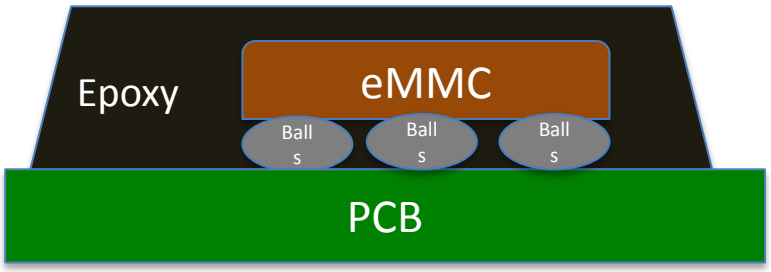
S5 mini

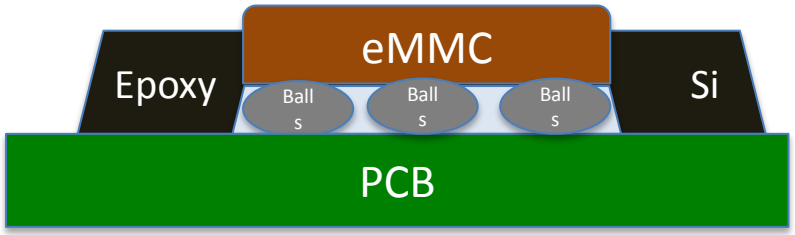


Welche Speichertypen dominieren?

- 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)

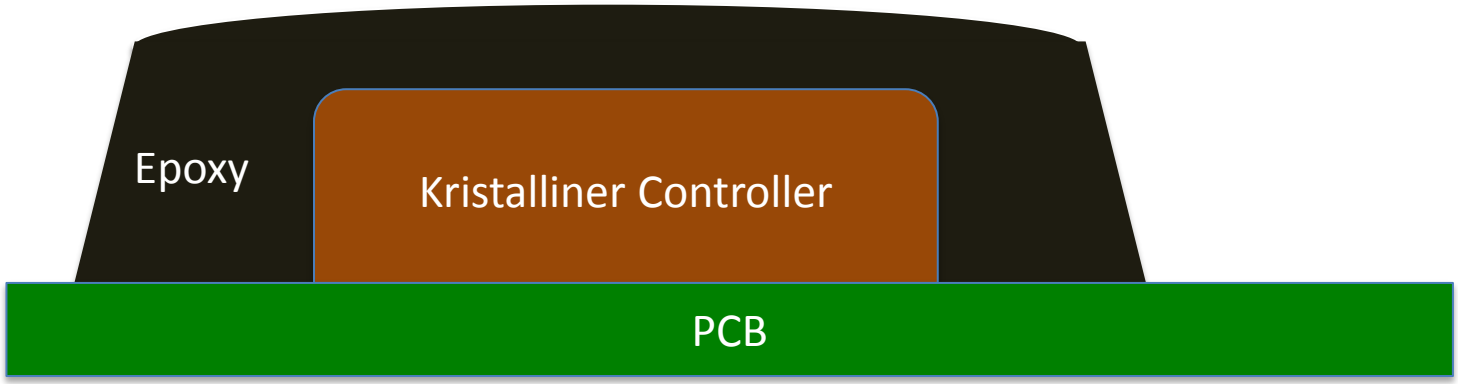
- eMMC und BGA Chips immer häufiger mit Epoxy vor Rissen geschützt
- eMMC mit Silikon umrahmt als weniger komplexer Schutz





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

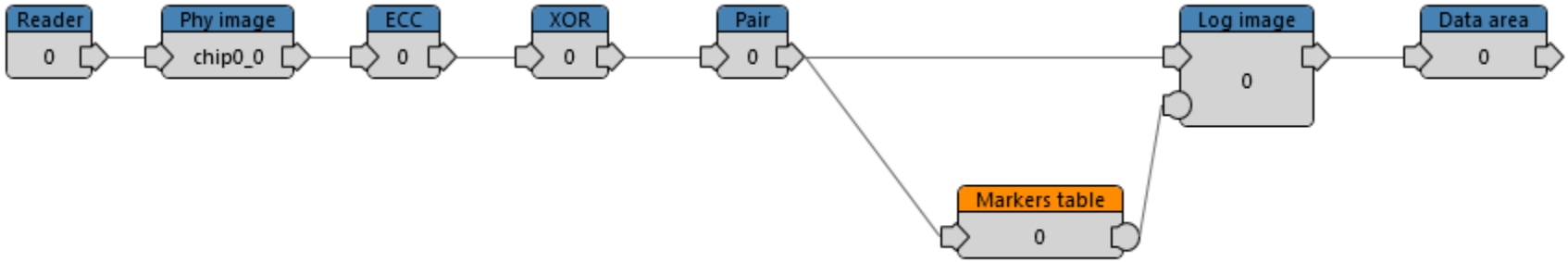
Wege zum Auslesen

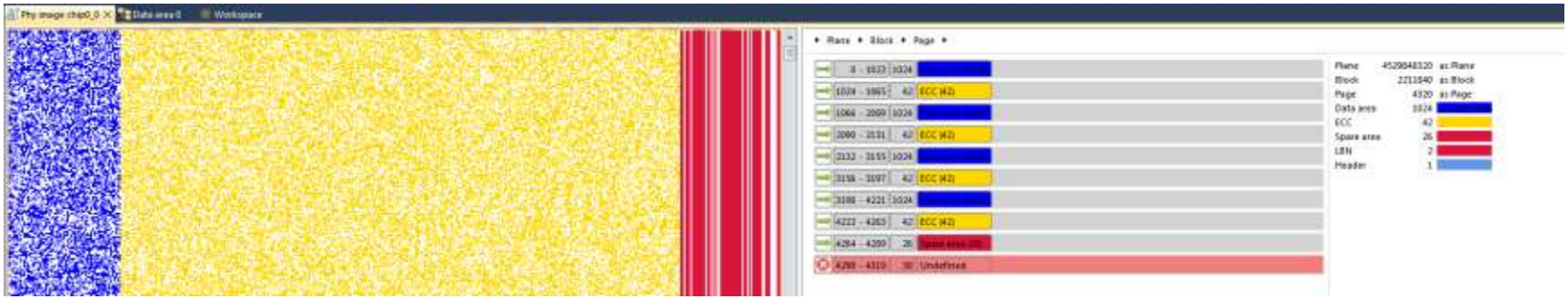
Adapter vs. Feinlöten

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

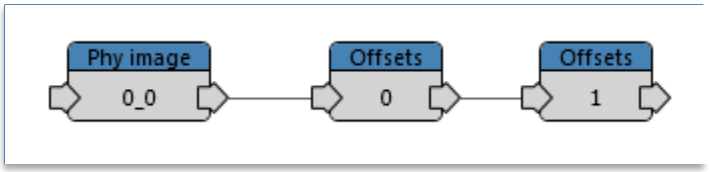
Manufaktur wird weiterhin überwiegen

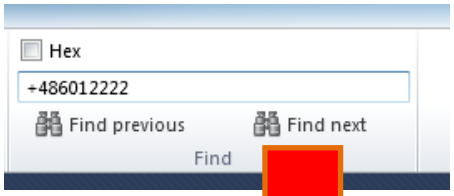
Wie sieht die Arbeit aus?

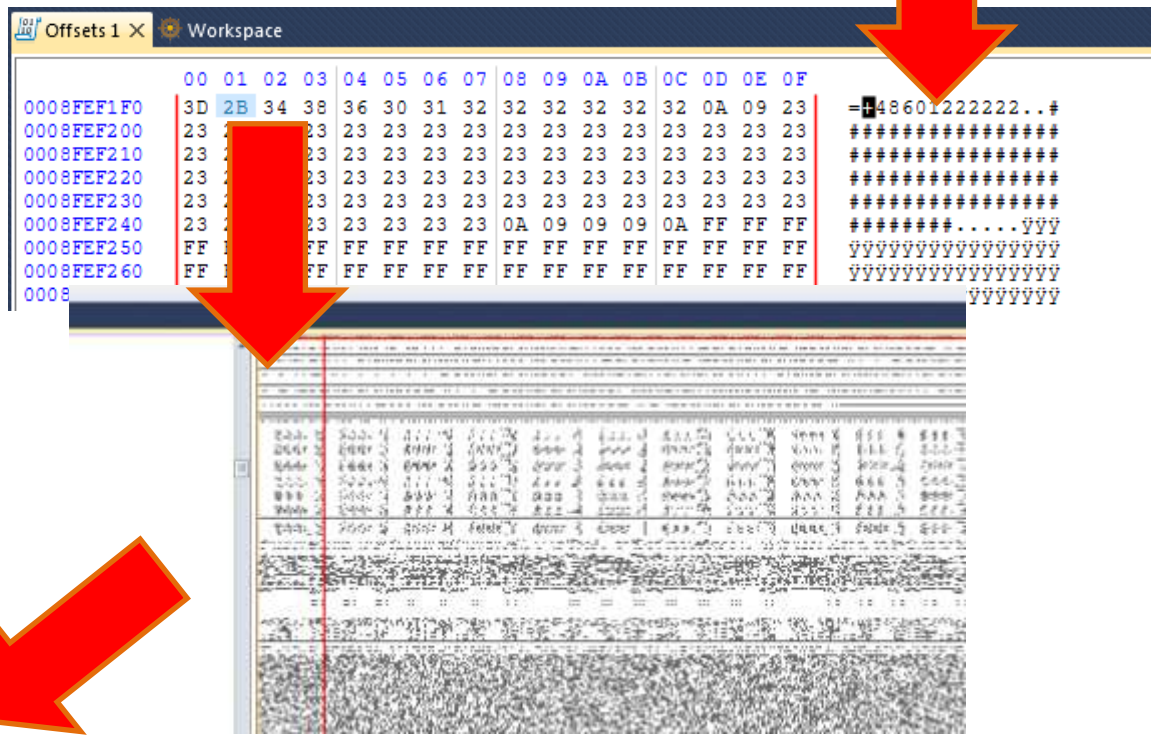




Beispiel – Sony Ericsson mit BGA137







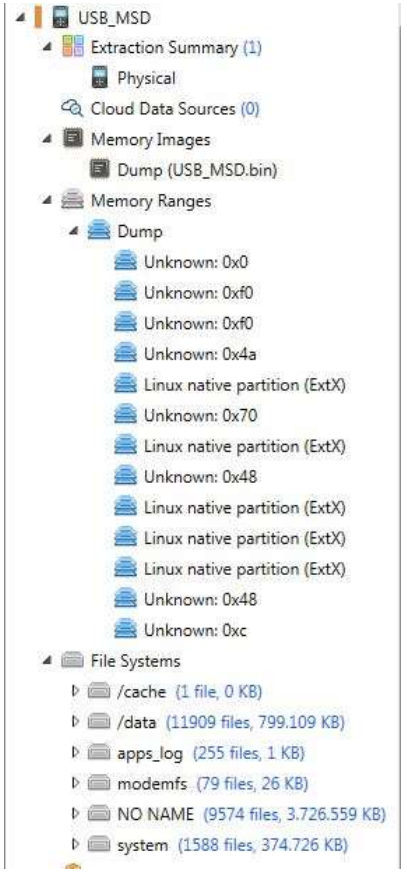
Byte position: 220; Row: 71657; Address: 151339804; Value: 11

Samsung Smartphones

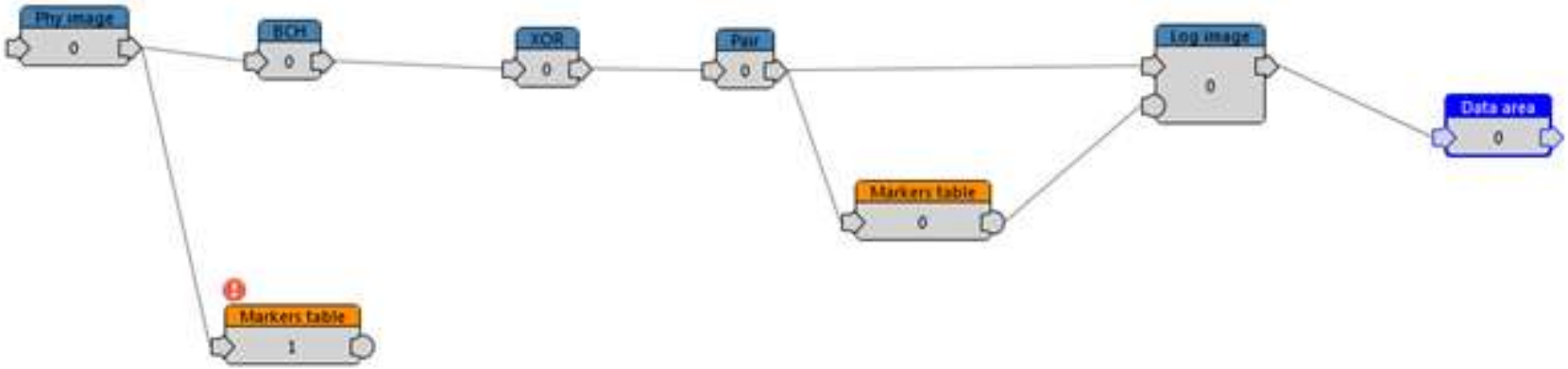
Chipoff ist bei nicht eingeschalter Verschlüsselung möglich!

z.B.

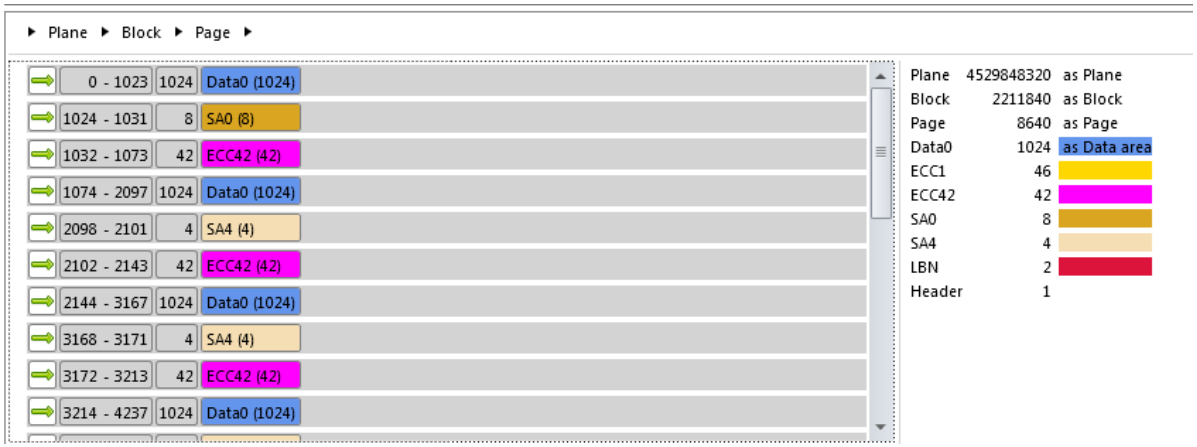
S4, S Duo, S5, …



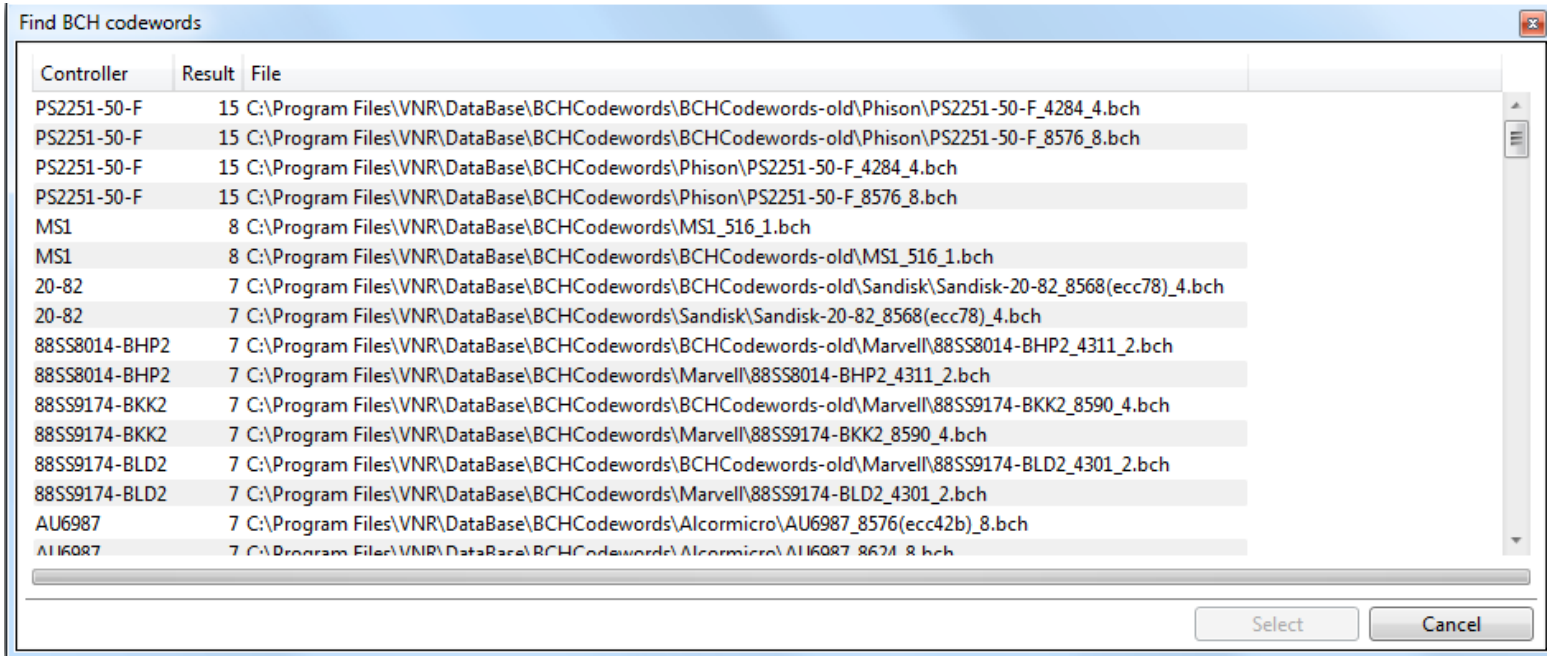
Von der Analyse zum Ergebnis



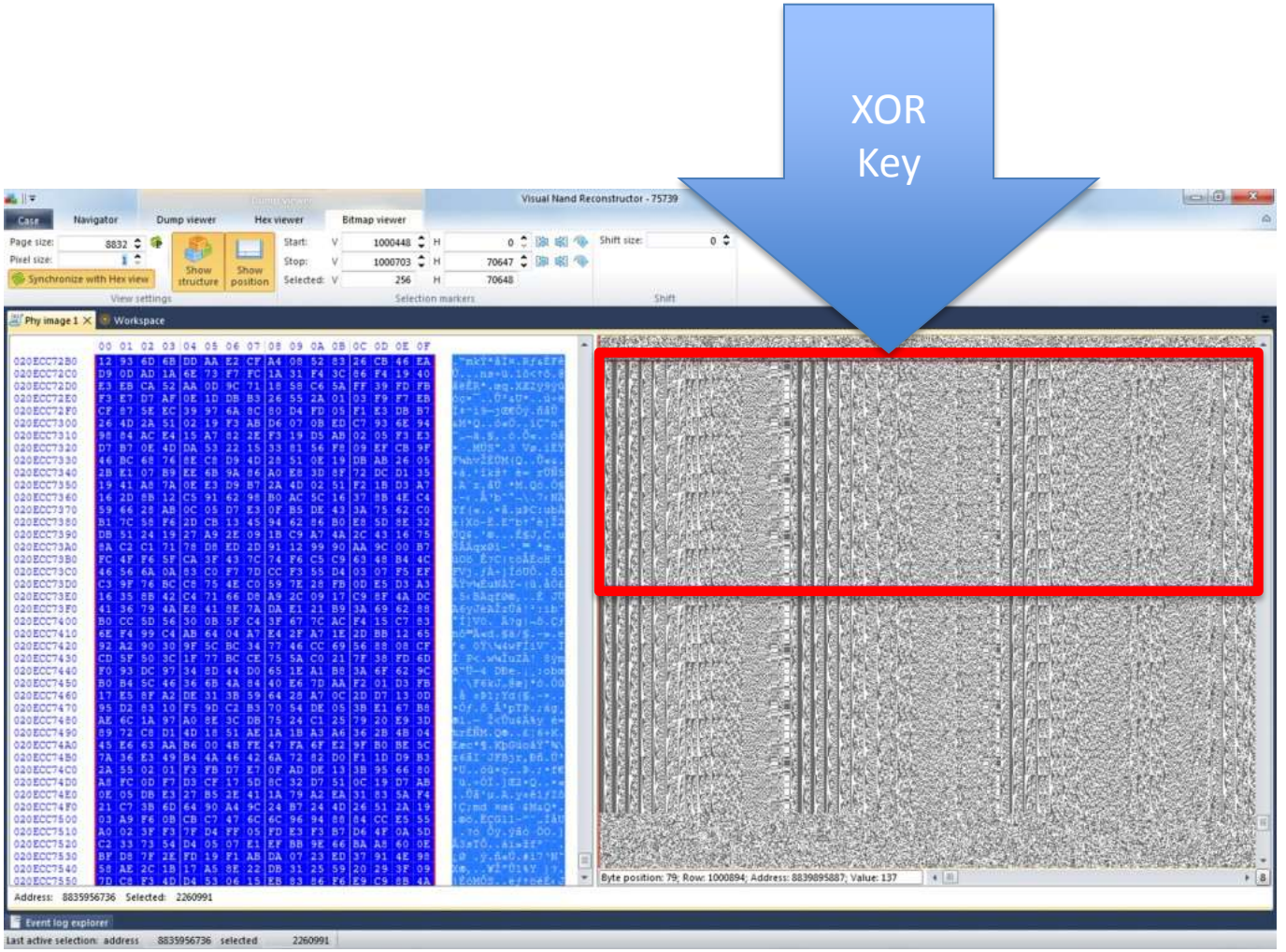
Analyse des Dumps



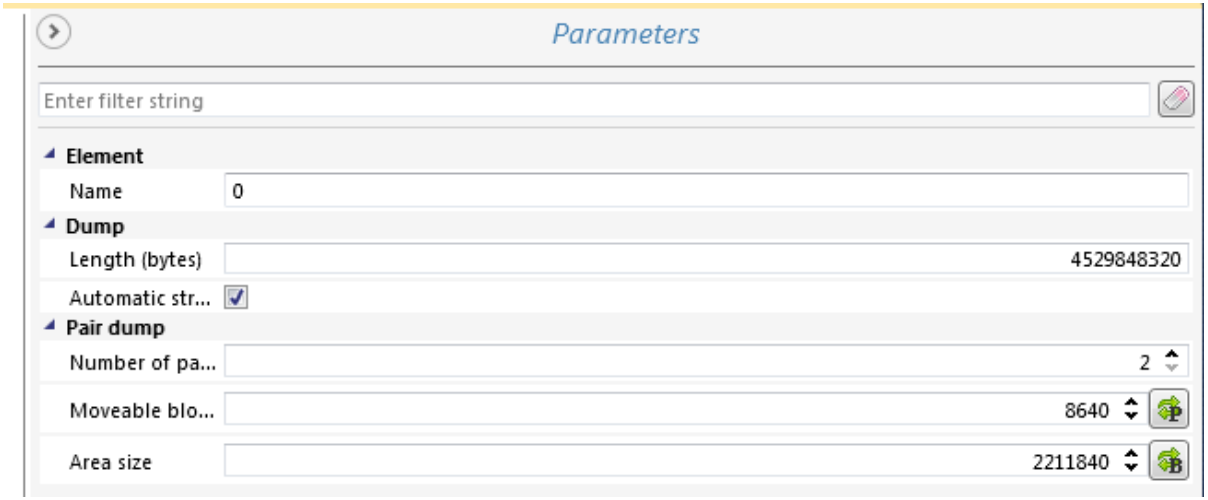
BCH Code finden oder recherchieren



XOR Key anwenden oder erarbeiten

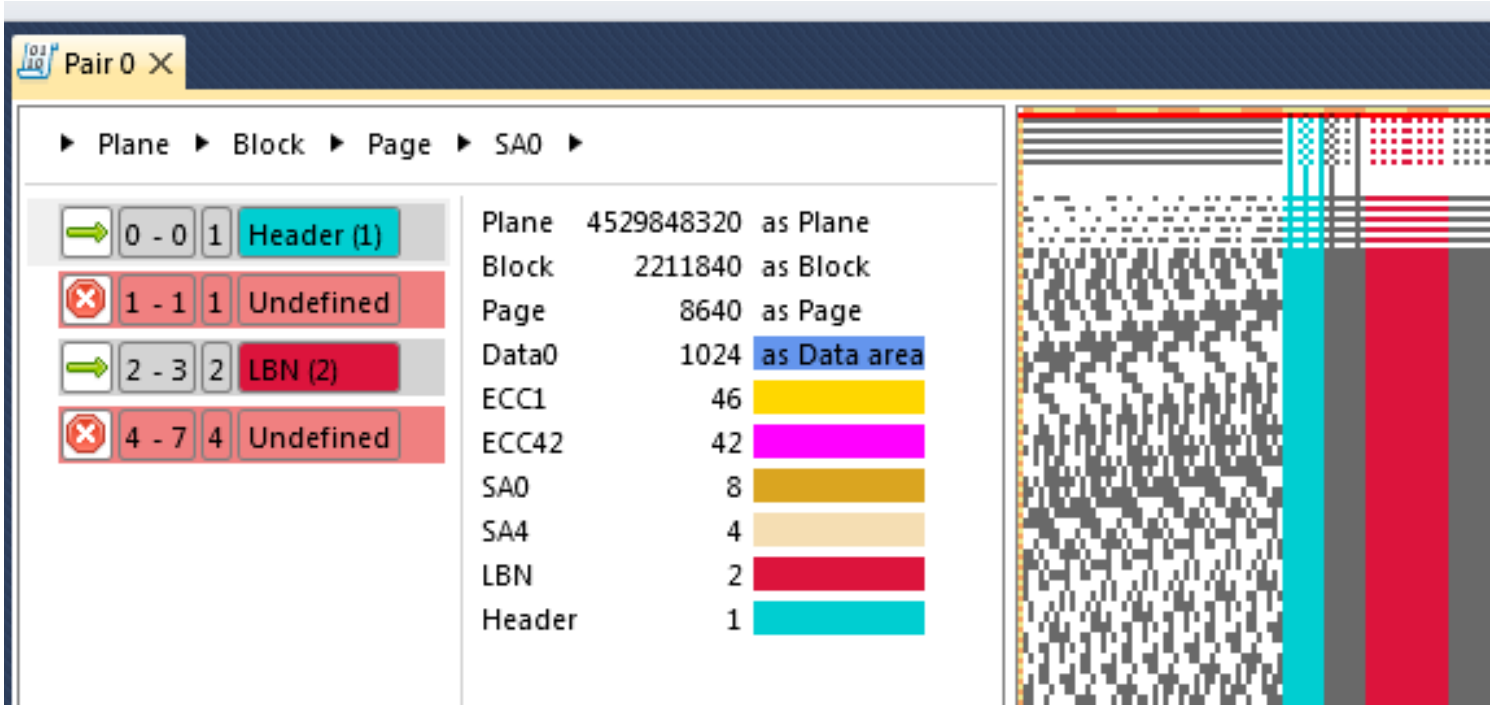


Pair – Raid 0 Daten zusammenführen

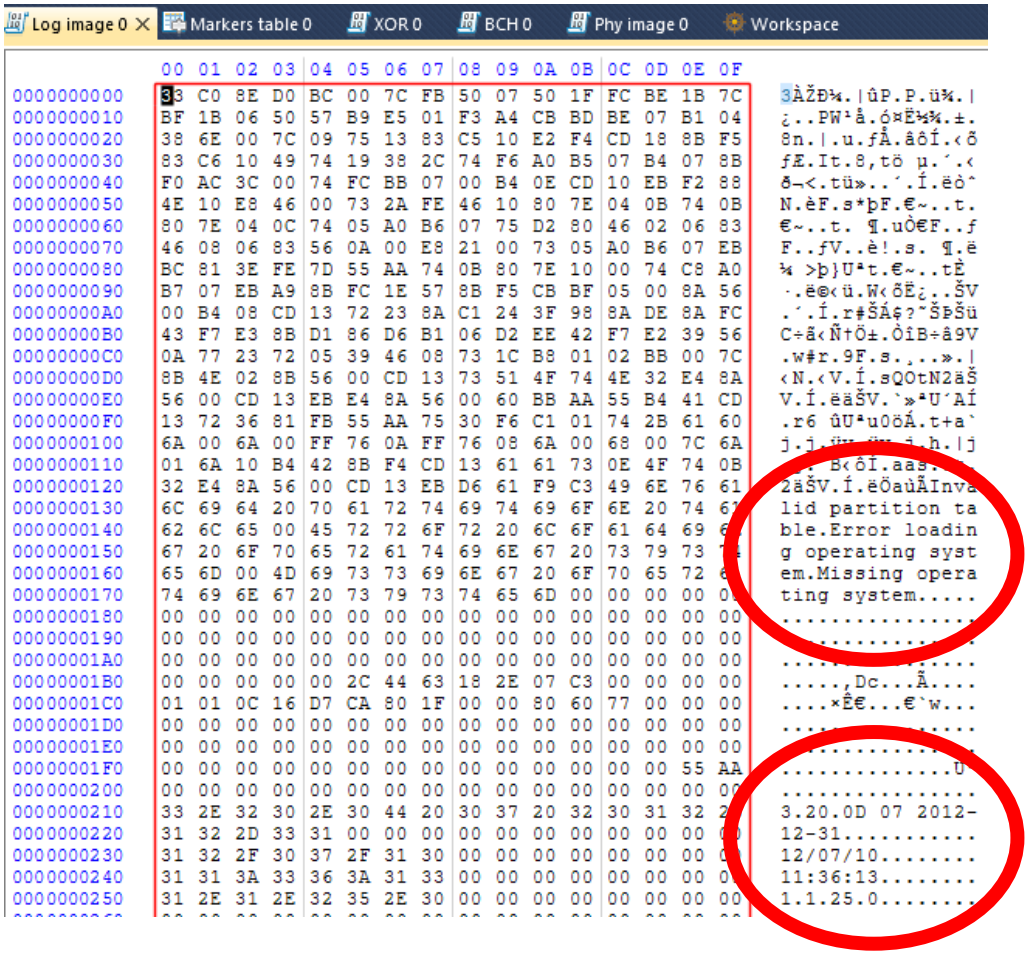


Markers Table

Header sowie LBN finden und kennzeichnen



Logical Image



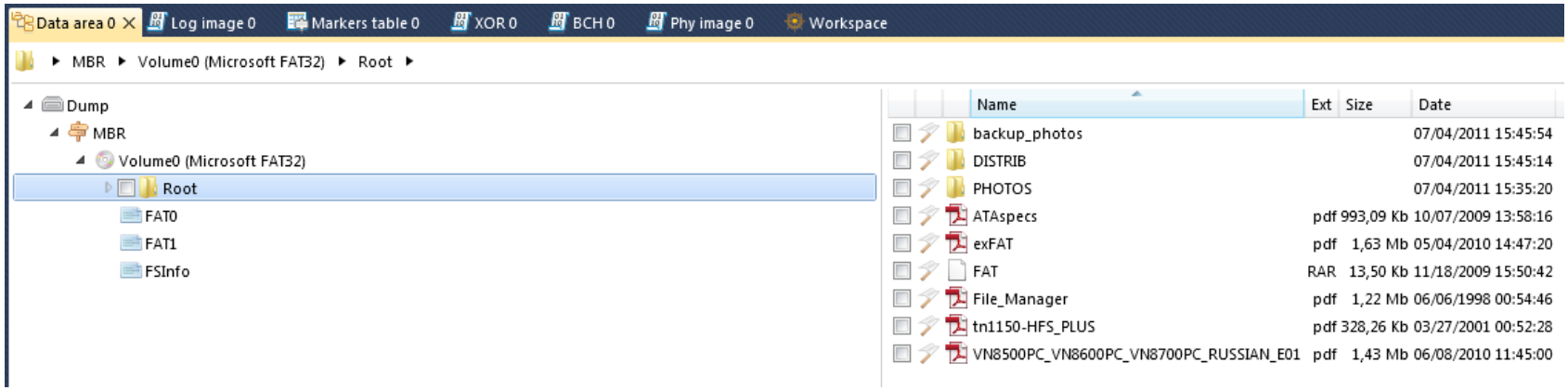
Daten werden auch in Hex lesbar

und

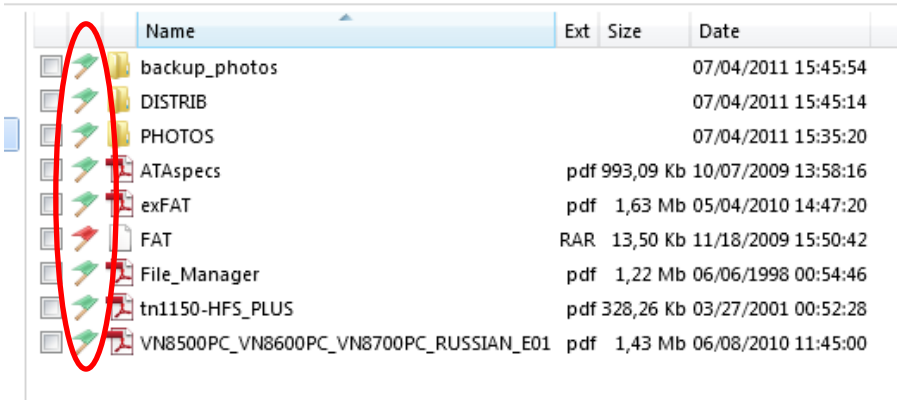
sind nicht mehr zerstückelt

Dump Folder Structure

- Am Ende können Dateien und Verzeichnisse sichtbar gemacht werden.



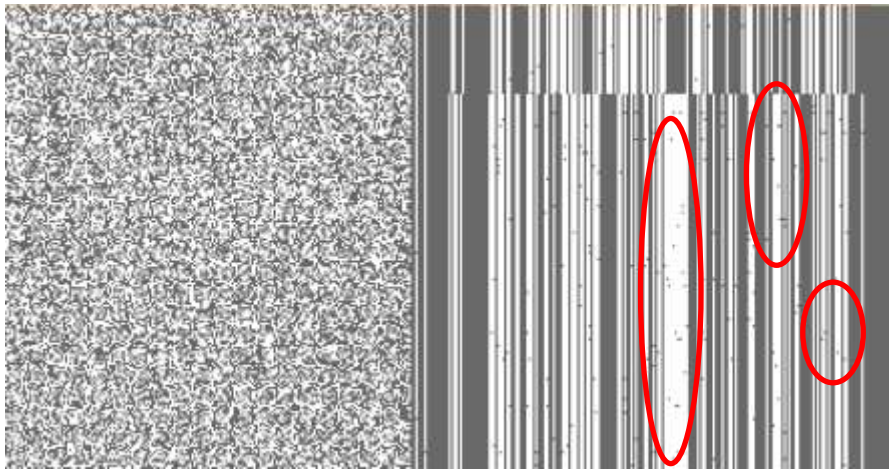
- Auch eine Header Prüfung ist möglich



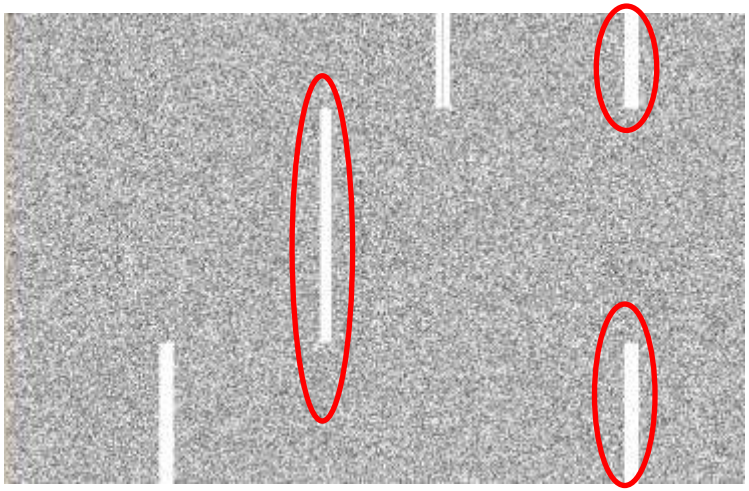
Problemlösungen

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

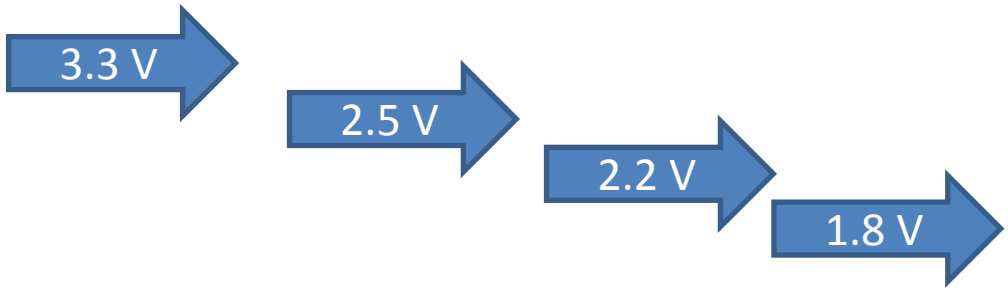
Bit Errors (sehen aus wie schlechte Pixel)

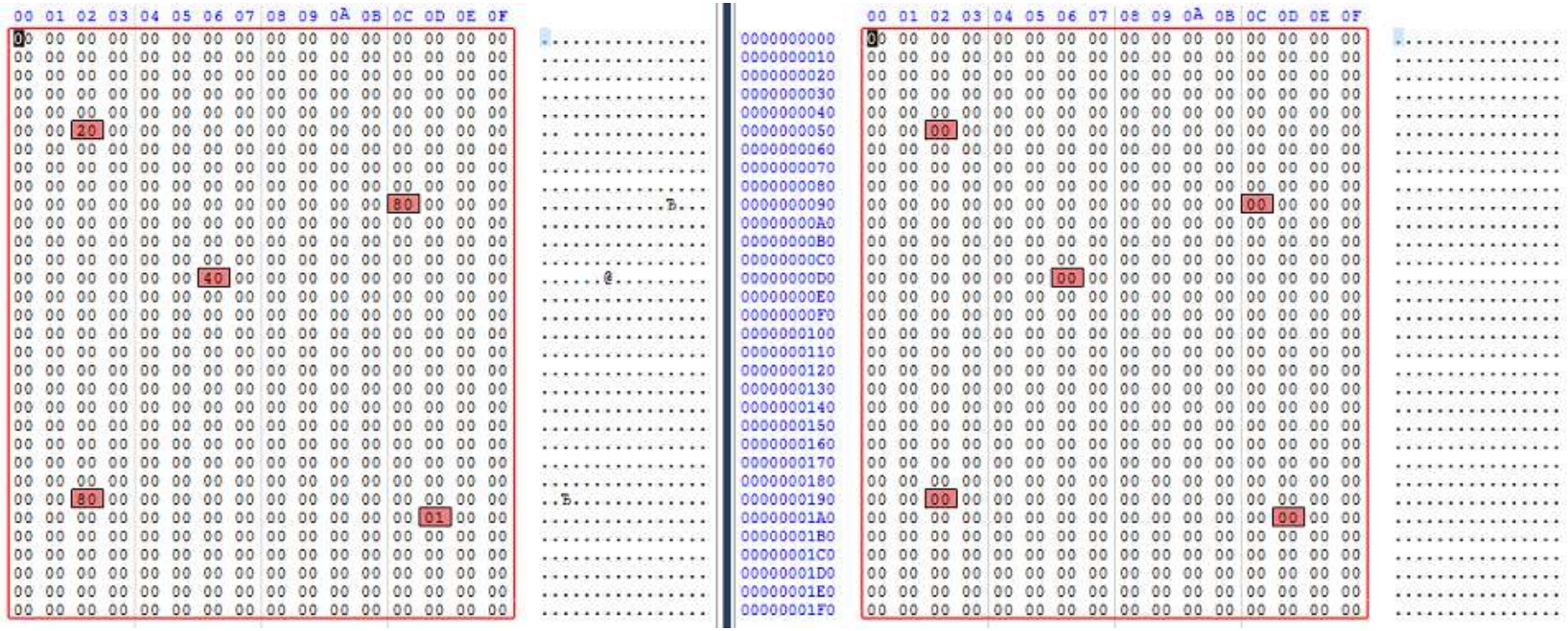


Bad Columns (Herstelldefekte)



Flexible Einstellung senkt Datenfehler

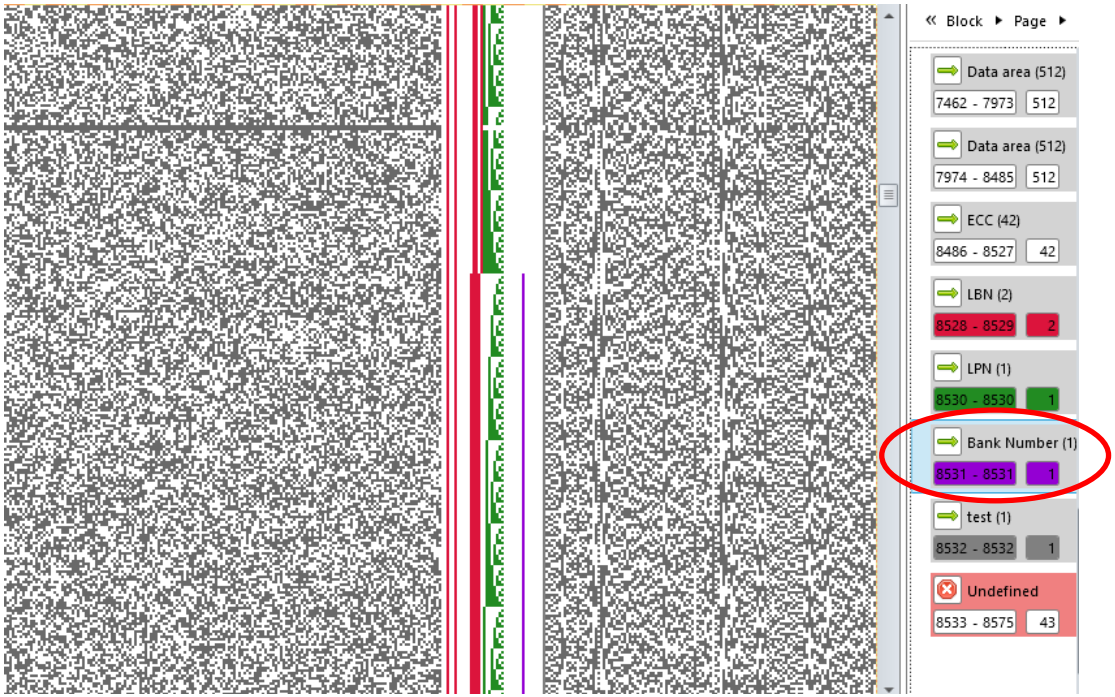




Bank Number

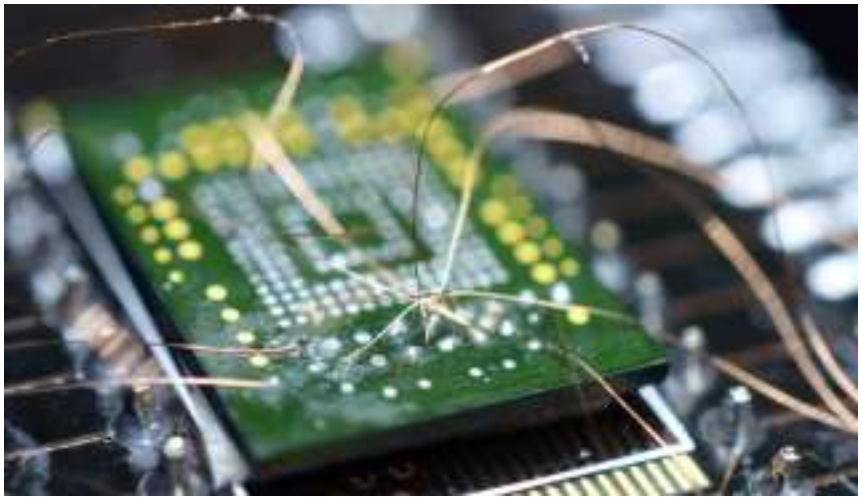
90% der Controller verwenden keine Bank Nummer.

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

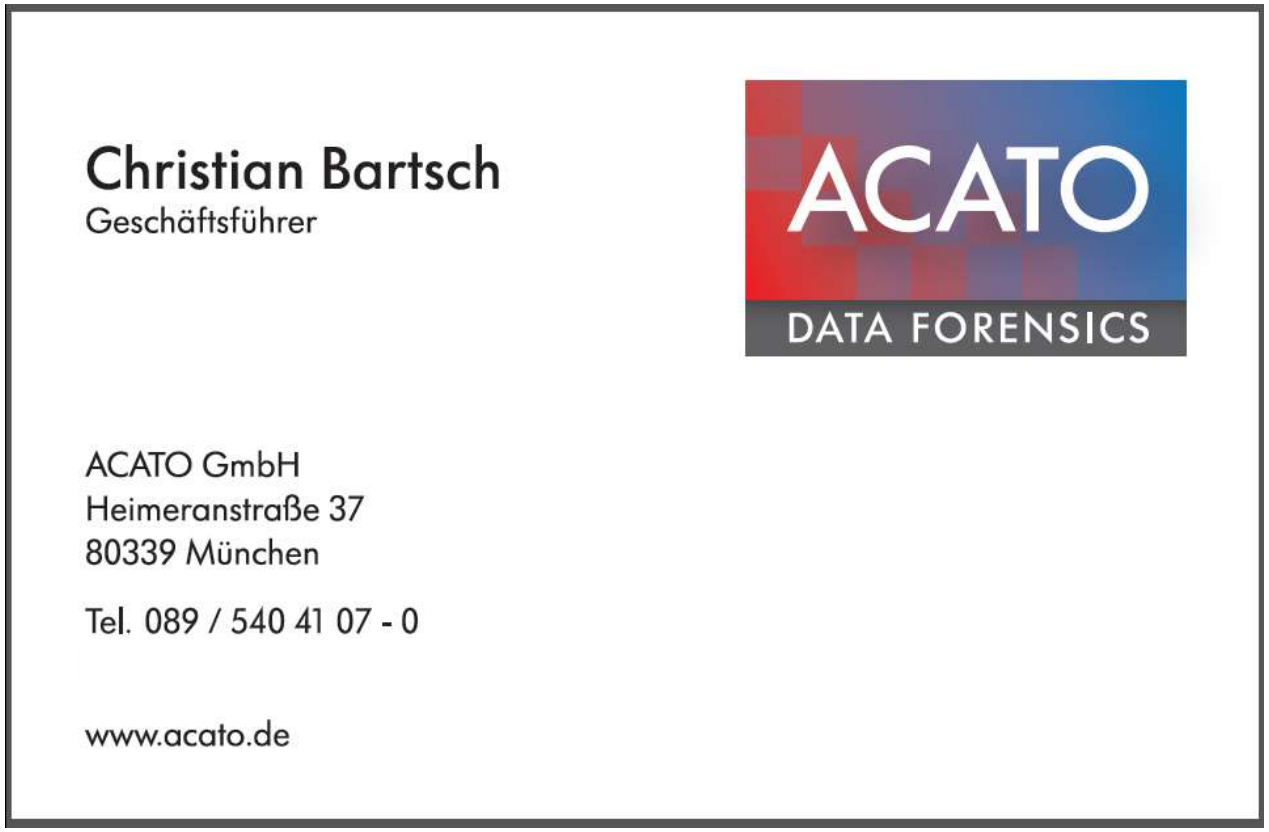
Dumps muss man analysieren und umwandeln für weitere forensische Auswertung.

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
DATA FORENSICS
ACATO GmbH
Heimeranstraße 37
80339 München
Tel. 089 / 540 41 07 - 0
www.acato.de