

Vehicle forensics, IoT and embedded file systems

Sasha Sheremetov, Rusolut

Mercedes AMG C43 (real case)



Multimedia Interface Control Unit



Mercedes-Benz A 222 900 48 19 /001

Hardware for Enhanced Remote-, Mobility- & Emergency Services

Model: HERMES 1.5
Version: LTE NAFTA
Type No: M197
WLAN - MAC: 2CDCADF
NAD SW: 11.787.01.00.1419
IMEI: 354189082
ICCID: 8901170427250
12V === 0.5A

ID: 0700 A 222 901 82 06 ZGS(HW): 001 17/37
EC: 100 A 222 902 72 18 ZGS(SW): 001 18/03

Serial No.: J263

Date of Manufacture: 2018/10/10

Q01

IC: 6434A - HERMES2

contains IC: 6369A - ME919BS567A

THE PRODUCT COMPLIES WITH DHHS RULES 21 CFR
SUBCHAPTER J APPLICABLE TO THE DATE OF MANUFACTURE.

FCC ID: T8GHERMES2

contains FCC ID: QISME919BS - 567A

THIS DEVICE COMPLIES WITH PART 15 OF THE FCC RULES AND INDUSTRY
CANADA LICENCE - EXEMPT RSS STANDARD(S). OPERATION IS SUBJECT
TO THE FOLLOWING TWO CONDITIONS:

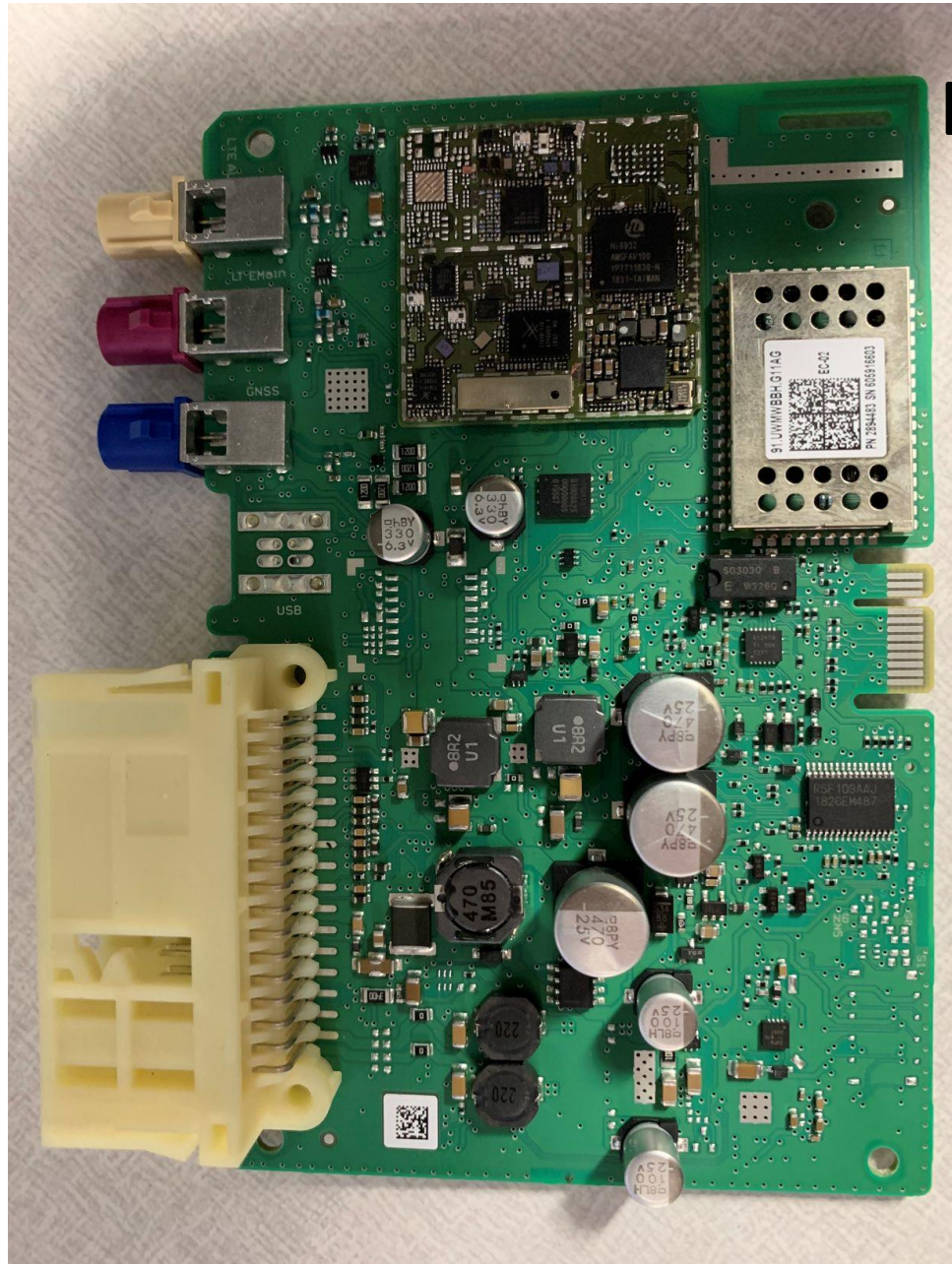
- (1) THIS DEVICE MAY NOT CAUSE HARMFUL INTERFERENCE, AND
- (2) THIS DEVICE MUST ACCEPT ANY INTERFERENCE RECEIVED,
INCLUDING INTERFERENCE THAT MAY CAUSE UNDESIRED OPERATION.

Harman Becker Automotive Systems GmbH
Becker - Göring - Straße 16
76307 Karlsbad, Germany
Manufactured in Hungary

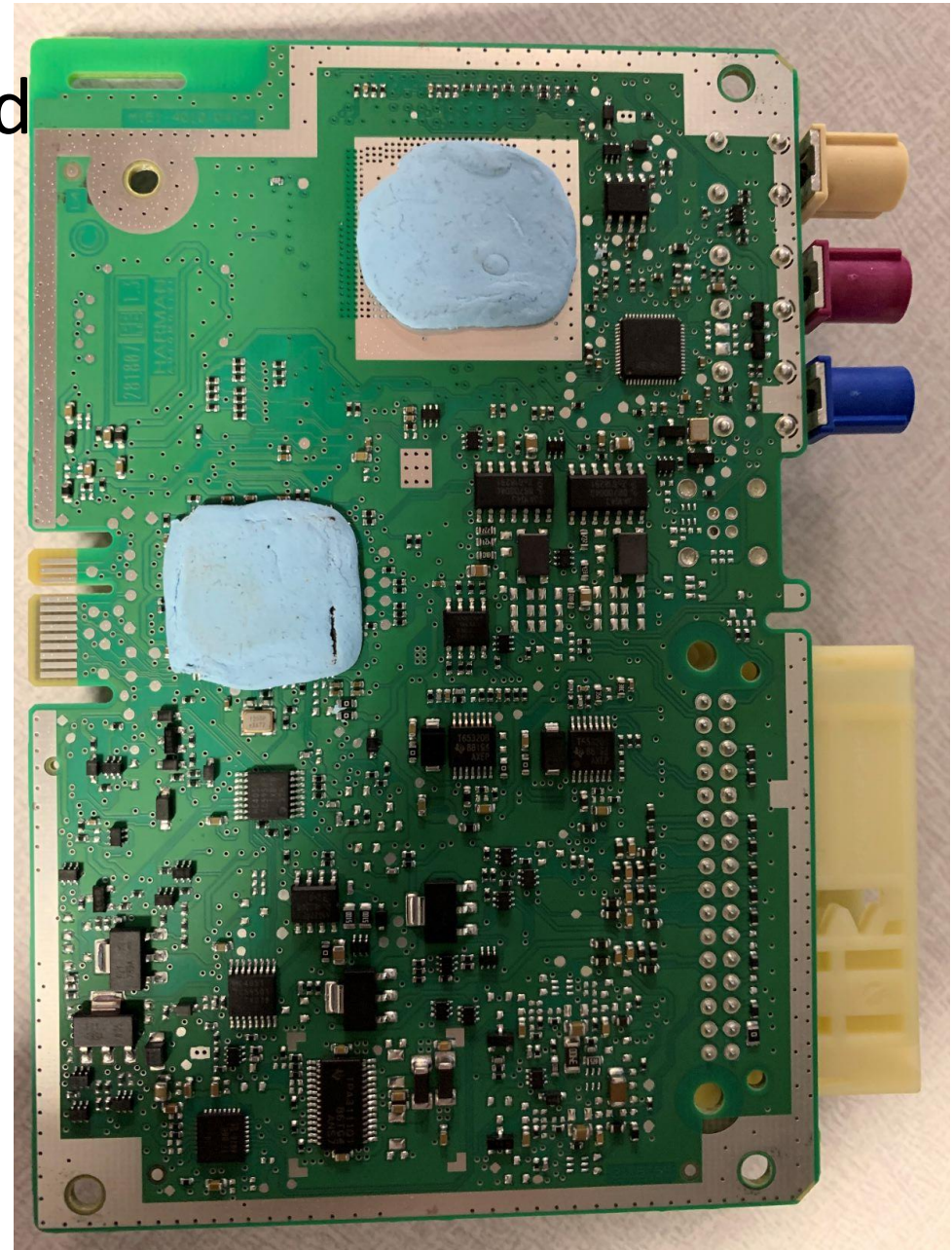


M197J80J263

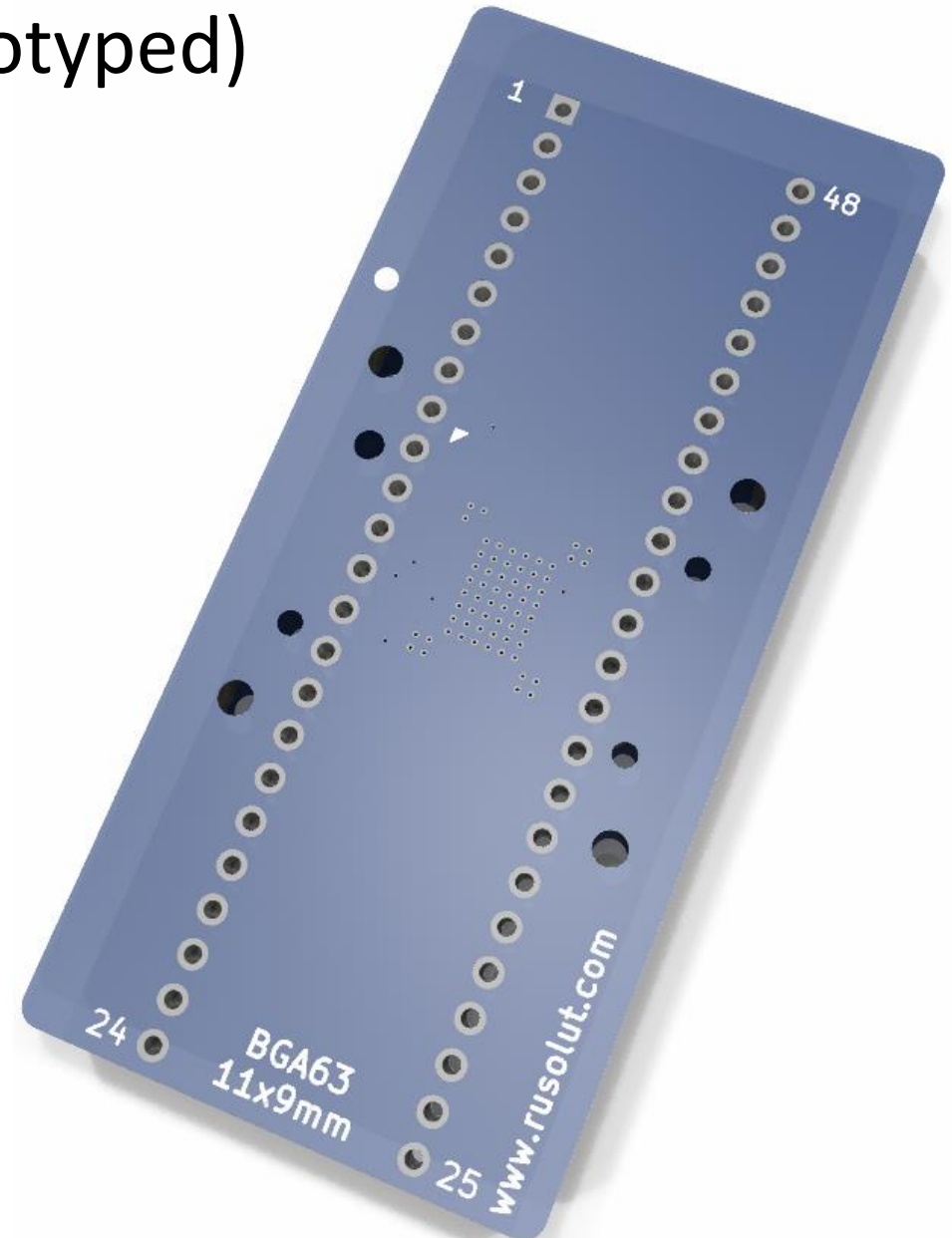
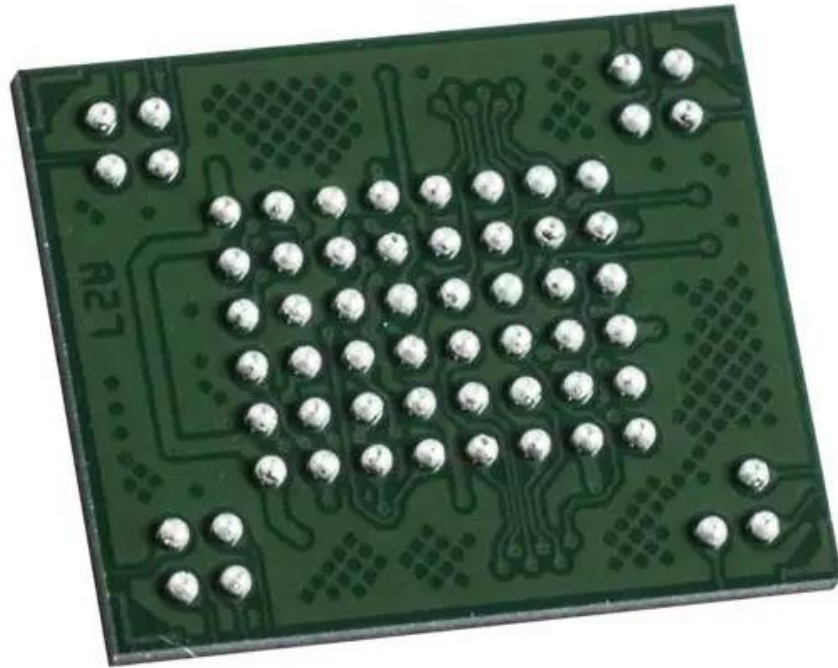




Board



BGA63 (prototyped)



Dump processing

Workspace X

Elements

Dump operations

Block list operations

Other

- R Reader
- PI Physical image
- BCR Bad byte col. remover
- bBCR Bad bit col. remover
- BCH ECC
- I Inversion
- X XOR
- P Pair
- U Unite
- O Offsets
- LI Logical image

Hide AI-powered

- X AU XOR
- X CBM XOR
- X FC XOR
- X IS XOR
- X ITE XOR
- X SM XOR

Workflow diagram:

```
graph LR; Reader[Reader 0] --> PhyImage[Phy image Chip0_0_0]; PhyImage --> ECC[ECC 0]; ECC --> BCR[BCR 0];
```

Warning icon above ECC step.

ObjID:
305 - Last valid time
408 - GPS fixes
402 - WiFi usage time

Yet Another Flash File System. Literally. YAFFS2

Case Yaffs parser

Meta data offset: 0 Sequence number offset: 2048 Byte count offset: 2060

Object Id offset: 2052 Block status offset: Read SA

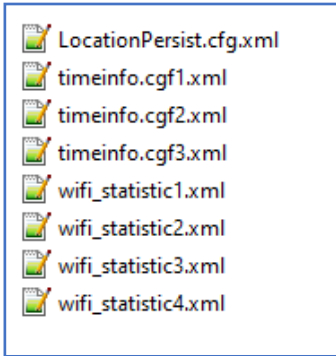
Chunk Id offset: 2056 Data status offset: Byte order Sync with dump

OOB positions

Use	Chur	Object Type	Object Id	Chunk Id	Sequence nur	Byte count	Parent	Name	Permissio	UID	GID	atime	mtime	ctime	File size	Address
✓	0x00	Data (0x00)	0x000401	0x000186	0x0000113F	0x0800										0x0010307700
✓	0x00	Data (0x00)	0x000401	0x000187	0x0000113F	0x0800										0x0010302CC0
✓	0x00	Data (0x00)	0x000401	0x000188	0x0000113F	0x0800										0x0010303500
✓	0x00	Data (0x00)	0x000401	0x000189	0x0000113F	0x0800										0x0010303D40
✓	0x00	Data (0x00)	0x000401	0x00018A	0x0000113F	0x0800										0x0010304580
✓	0x00	Data (0x00)	0x000401	0x00018B	0x0000113F	0x0618										0x0010304DC0
✓	0x80	File header (0x10)	0x000402	0x000001	0x0000ED27	0x010B	0x1	onoff.log	0x81B6	0x0	0x0	0x5C807E4B	0x5E51DBB8	0x5E51DBB8	0x10B	0x0010E8BC80
✓	0x80	File header (0x10)	0x000402	0x000201	0x000053A8	0x0000	0x201	OMCPersist.cfg	0x81A4	0x3F0	0x3F0	0x5685D031	0x5D7990F3	0x5D7990F3	0x0	0x001DF226C0
✓	0x80	File header (0x10)	0x000402	0x000201	0x000053A8	0x0000	0x201	OMCPersist.cfg	0x81A4	0x3F0	0x3F0	0x5685D031	0x5D7990F3	0x5D7990F3	0x0	0x001DF22F00
✓	0x80	File header (0x10)	0x000402	0x000201	0x000053A8	0x0225	0x201	OMCPersist.cfg	0x81A4	0x3F0	0x3F0	0x5685D031	0x5D7990F3	0x5D7990F3	0x225	0x001DF23F80
✓	0x80	File header (0x10)	0x000402	0x000401	0x000041D4	0x015C	0x401	wifi_statistic.xml	0x81B0	0x3E8	0x3E8	0x135	0x5D798944	0x5D798B9B	0x15C	0x001FE57000
✓	0x80	File header (0x10)	0x000402	0x000401	0x000041D4	0x0000	0x401	wifi_statistic.xml	0x81B0	0x3E8	0x3E8	0x135	0x5D798B9B	0x5D798B9B	0x0	0x001FE57840
✓	0x80	File header (0x10)	0x000402	0x000401	0x000041D4	0x0000	0x401	wifi_statistic.xml	0x81B0	0x3E8	0x3E8	0x135	0x5D798B9B	0x5D798B9B	0x0	0x001FE58080
✓	0x80	File header (0x10)	0x000402	0x000401	0x000041D4	0x0000	0x401	wifi_statistic.xml	0x81B0	0x3E8	0x3E8	0x135	0x5D798B9B	0x5D798B9B	0x0	0x001FE588C0
✓	0x80	File header (0x10)	0x000402	0x000401	0x000041D4	0x0000	0x401	wifi_statistic.xml	0x81B0	0x3E8	0x3E8	0x135	0x5D798B9B	0x5D798B9B	0x0	0x001FE59100
✓	0x80	File header (0x10)	0x000402	0x000401	0x000041D4	0x015D	0x401	wifi_statistic.xml	0x81B0	0x3E8	0x3E8	0x135	0x5D798B9B	0x5D798B9B	0x15D	0x001FE5A180
✓	0x80	File header (0x10)	0x000402	0x000401	0x000041D4	0x015D	0x401	wifi_statistic.xml	0x81B0	0x3E8	0x3E8	0x135	0x5D798B9B	0x5D798DF5	0x15D	0x001FE690C0
✓	0x80	File header (0x10)	0x000402	0x000401	0x000041D4	0x015D	0x401	wifi_statistic.xml	0x81B0	0x3E8	0x3E8	0x135	0x5D798B9B	0x5D798DF5	0x15D	0x001FE69900
✓	0x80	File header (0x10)	0x000402	0x000401	0x000041D4	0x0000	0x401	wifi_statistic.xml	0x81B0	0x3E8	0x3E8	0x135	0x5D798DF5	0x5D798DF5	0x0	0x001FE6A140
✓	0x80	File header (0x10)	0x000402	0x000401	0x000041D4	0x0000	0x401	wifi_statistic.xml	0x81B0	0x3E8	0x3E8	0x135	0x5D798DF5	0x5D798DF5	0x0	0x001FE6A980
✓	0x80	File header (0x10)	0x000402	0x000401	0x000041D4	0x0000	0x401	wifi_statistic.xml	0x81B0	0x3E8	0x3E8	0x135	0x5D798DF5	0x5D798DF5	0x0	0x001FE6B1C0
✓	0x80	File header (0x10)	0x000402	0x000401	0x000041D4	0x0000	0x401	wifi_statistic.xml	0x81B0	0x3E8	0x3E8	0x135	0x5D798DF5	0x5D798DF5	0x0	0x001FE6BA00
✓	0x80	File header (0x10)	0x000402	0x000401	0x000041D4	0x015D	0x401	wifi_statistic.xml	0x81B0	0x3E8	0x3E8	0x135	0x5D798DF5	0x5D798DF5	0x15D	0x001FE6CA80
✓	0x80	File header (0x10)	0x000402	0x000401	0x000041D4	0x015D	0x401	wifi_statistic.xml	0x81B0	0x3E8	0x3E8	0x135	0x5D798DF5	0x5D799050	0x15D	0x001FE6D2C0
✓	0x80	File header (0x10)	0x000402	0x000401	0x000041D4	0x015D	0x401	wifi_statistic.xml	0x81B0	0x3E8	0x3E8	0x135	0x5D798DF5	0x5D799050	0x15D	0x001FE6DB00
✓	0x80	File header (0x10)	0x000402	0x000401	0x000041D4	0x0000	0x401	wifi_statistic.xml	0x81B0	0x3E8	0x3E8	0x135	0x5D799050	0x5D799050	0x0	0x001FE6E340
✓	0x80	File header (0x10)	0x000402	0x000401	0x000041D4	0x0000	0x401	wifi_statistic.xml	0x81B0	0x3E8	0x3E8	0x135	0x5D799050	0x5D799050	0x0	0x001FE6EB80
✓	0x80	File header (0x10)	0x000402	0x000401	0x000041D4	0x0000	0x401	wifi_statistic.xml	0x81B0	0x3E8	0x3E8	0x135	0x5D799050	0x5D799050	0x0	0x001FE6F3C0
✓	0x80	File header (0x10)	0x000402	0x000401	0x000041D4	0x0000	0x401	wifi_statistic.xml	0x81B0	0x3E8	0x3E8	0x135	0x5D799050	0x5D799050	0x0	0x001FE6FC00
✓	0x80	File header (0x10)	0x000402	0x000401	0x000041D4	0x015D	0x401	wifi_statistic.xml	0x81B0	0x3E8	0x3E8	0x135	0x5D799050	0x5D799050	0x15D	0x001FE70C80
✓	0x80	File header (0x10)	0x000402	0x000401	0x000041D4	0x015D	0x401	wifi_statistic.xml	0x81B0	0x3E8	0x3E8	0x135	0x5D799050	0x5D799084	0x15D	0x001FE714C0
✓	0x80	File header (0x10)	0x000402	0x000401	0x000041D4	0x015D	0x401	wifi_statistic.xml	0x81B0	0x3E8	0x3E8	0x135	0x5D799050	0x5D799084	0x15D	0x001FE71D00
✓	0x80	File header (0x10)	0x000402	0x000401	0x000041D4	0x0000	0x401	wifi_statistic.xml	0x81B0	0x3E8	0x3E8	0x135	0x5D799084	0x5D799084	0x0	0x001FE72540
✓	0x80	File header (0x10)	0x000402	0x000401	0x000041D4	0x0000	0x401	wifi_statistic.xml	0x81B0	0x3E8	0x3E8	0x135	0x5D799084	0x5D799084	0x0	0x001FE72D80
✓	0x80	File header (0x10)	0x000402	0x000401	0x000041D4	0x0000	0x401	wifi_statistic.xml	0x81B0	0x3E8	0x3E8	0x135	0x5D799084	0x5D799084	0x0	0x001FE735C0

```
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
0010ED26C0 32 30 31 39 2D 30 33 2D 30 37 20 30 32 3A 31 33 2019-03-07 02:13
0010ED26D0 3A 33 31 20 5B 31 33 2E 30 36 34 5D 20 47 41 55 :31 [13.064]GAU
0010ED26E0 3A 63 79 63 6C 65 3C 39 3E 3A 73 65 74 44 54 43 :cycle<9>:setDTC
0010ED26F0 57 61 74 63 68 64 6F 67 52 65 73 65 74 20 57 55 WatchdogReset WU
0010ED2700 52 3C 30 78 32 30 30 30 3E 20 6C 61 73 74 20 65 R<0x2000> last e
0010ED2710 6E 74 72 79 3A 20 3C 3E 0A 32 30 32 30 2D 30 32 ntry: <>.2020-02
0010ED2720 2D 32 33 20 30 31 3A 35 36 3A 30 38 20 5B 31 33 -23 01:56:08 [13
0010ED2730 2E 31 38 39 5D 20 47 41 55 3A 63 79 63 6C 65 3C .189] GAU:cycle<
0010ED2740 33 39 3E 3A 73 65 74 44 54 43 57 61 74 20 65 39>:setDTCWatchd
0010ED2750 6F 67 52 65 73 65 74 20 57 55 52 3C 30 78 32 30 ogReset WUR<0x20
0010ED2760 30 30 3E 20 6C 61 73 74 20 65 6E 74 72 79 3A 20 00> last entry:
0010ED2770 3C 32 30 31 39 2D 30 33 2D 30 37 20 30 32 3A 31 <2019-03-07 02:1
0010ED2780 33 3A 33 31 20 5B 31 33 2E 30 36 34 5D 20 47 41 3:31 [13.064] GA
0010ED2790 55 3A 63 79 63 6C 65 3C 39 3E 3A 73 65 74 44 54 U:cycle<9>:setDT
0010ED27A0 43 57 61 74 63 68 64 6F 67 52 65 73 65 74 20 57 CWatchdogReset W
0010ED27B0 55 52 3C 30 78 32 30 30 3E 20 6C 61 73 74 20 57 UR<0x2000> last
0010ED27C0 65 6E 74 72 79 3A 20 3C 3E 3E 0A 00 00 00 00 00 entry: <>.....
0010ED27D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0010ED27E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0010ED27F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0010ED2800 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0010ED2810 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0010ED2820 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0010ED2830 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0010ED2840 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0010ED2850 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0010ED2860 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0010ED2870 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0010ED2880 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0010ED2890 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0010ED28A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0010ED28B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0010ED28C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0010ED28D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0010ED28E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0010ED28F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0010ED2900 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0010ED2910 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0010ED2920 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0010ED2930 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0010ED2940 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0010ED2950 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0010ED2960 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0010ED2970 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0010ED2980 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
```

Files extracted from YAFFS2



```
LocationPersist.cfg.xml
LocationDataSaved
{
  Latitude 1682663912
  Longitude 784841424
  Velocity 1
  Heading 274
  LocAttributes 274.39999
  EllipsoidHeigh 0
  Altitude 1216
  VisibleSatellites 12
  TrackingSatellites 0
  Fix 1
  GPSVdop 0
  GPSHdop 0
  GPSPdop 0
  Timestamp 0
  ValidationFlag true
  Year 2019
  Month 9
  Day 12
  Hour 0
  Minutes 24
  Seconds 2
  history_size 9
  Latitude_0 1682671199
  Longitude_0 784843863
  Velocity_0 0
  Heading_0 324
  LocAttributes_0 324.70001
  EllipsoidHeigh_0 0
  Altitude_0 1217
  VisibleSatellites_0 12
  TrackingSatellites_0 12
  Fix_0 4
  GPSVdop_0 0
  GPSHdop_0 0
  GPSPdop_0 0
  Year_0 2019
  Month_0 9
  Day_0 12
  Hour_0 0
  Minutes_0 23
  Seconds_0 34
}
```

```
wifi_statistic1.xml
<?xml version="1.0" encoding="UTF-8"?>
<config>
  <total_connected_time>904902</total_connected_time>
  <total_rx>191936195</total_rx>
  <total_tx>124303838</total_tx>
  <total_flow>316240033</total_flow>
  <curr_connected_time>3006</curr_connected_time>
  <curr_rx>738407</curr_rx>
  <curr_tx>437491</curr_tx>
  <curr_flow>1175898</curr_flow>
</config>
```

```
timeinfo.cgf1.xml
TimeInfo
{
  version 1
  deltaValue 4294945688
  lastValidTime 1567867559
}
```


BMW 3 F30 (online scrap yard)



Multimedia Unit

Garantie Magneti Marelli

SNR: 0002557
Type: NAV ECE 010F 14
CE XXXX

Manufactured in Slovakia by: Model No. NAV	S-ID
SW ID: F020-17-03-582	MAC-adr:
Accession No: CO-410-031-6	Version: ECE Date: 18.05.17

HIP: 0ABA66P4E157
MM pn: 503551GQ2114
HW: 004.003.003

191184 10
B1/VV
6512

CRIN: MMA-01DF-H-2557470

CI 8 792 157 01

MAGNETI MARELLI CE 0560 E24 10R-05 164B

Magneti Marelli S.p.A.
Product: EN2
12V 15A

Aprobado CNC: C-14777
CMIIT TD: 2015DJ3829
Includes transmitter
FCC ID: RX2EN2
IC 4983A-EN2

TRA/TA: TRA/TA-R/2644/15
DOB0134

ETA: NR-ETA/2144

Complies with
IDA standards
DA101586

IFT: RCPBEN15-1000

NOM NTC

CCAN15LP0310T9

TA No: DRQ-D-MAJU-02-2011 111083-LPD-30344

CLASS 1 LASER PRODUCT

TRA REGISTERED No: ER40BB1/15
DEALER No: DA0110016/13
MAGNETI MARELLI S.P.A.

201-150248

IC 4983A-EN2

TA 2015/2015 APPROVED

ZICTA

2719-15-0386

1024

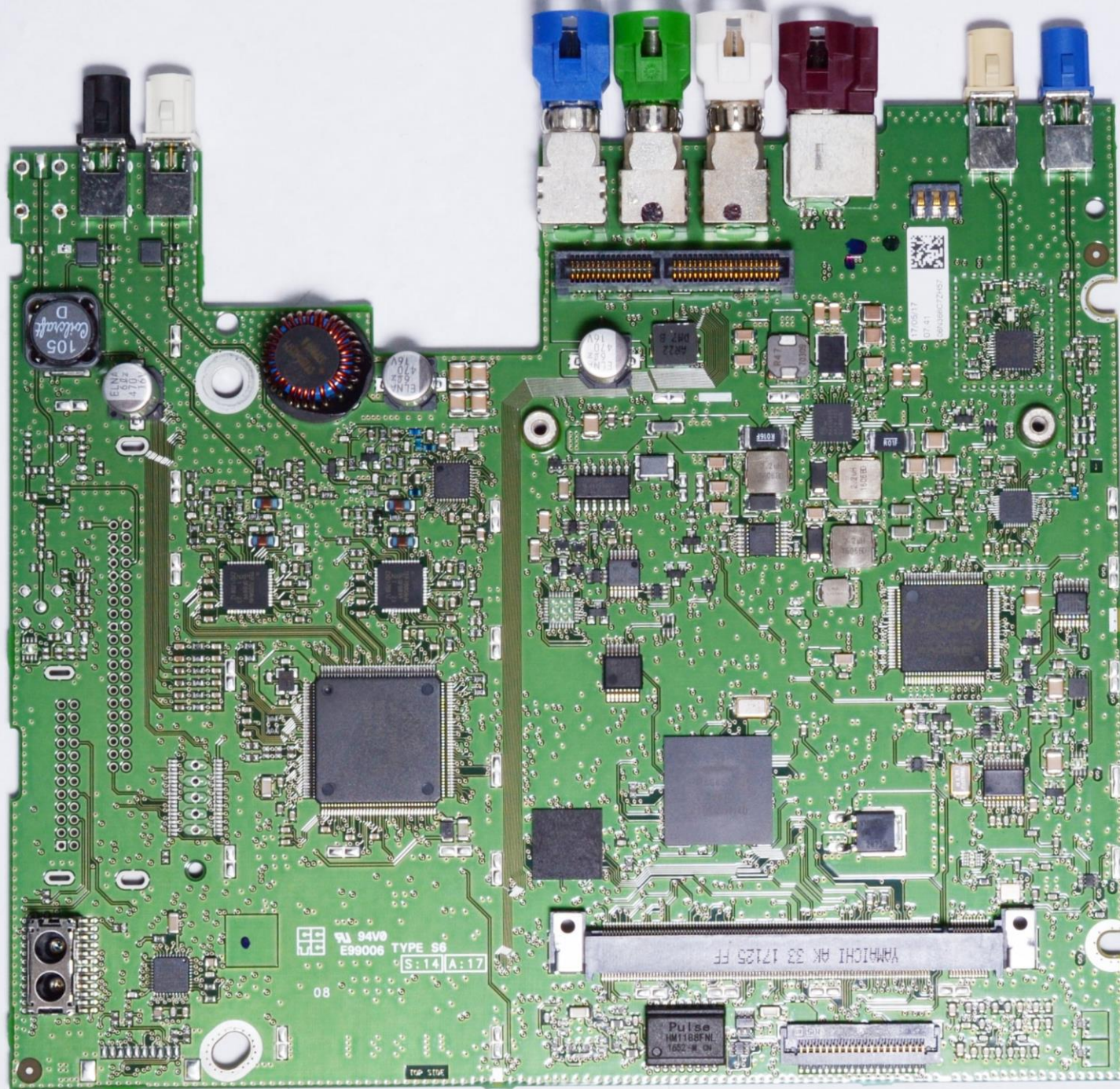
Este equipamento opera em caráter secundário, isto é, não tem direito a proteção contra interferência prejudicial, mesmo de estações do mesmo tipo, e não pode causar interferência a sistemas operando em caráter primário.

HD Radio Technology manufactured under license from IDigit Digital Corporation, U.S. and foreign Patents. HD Radio and the HD, HD Radio and "Arc" logos are proprietary Trade Marks of IDigit Digital, Corp.

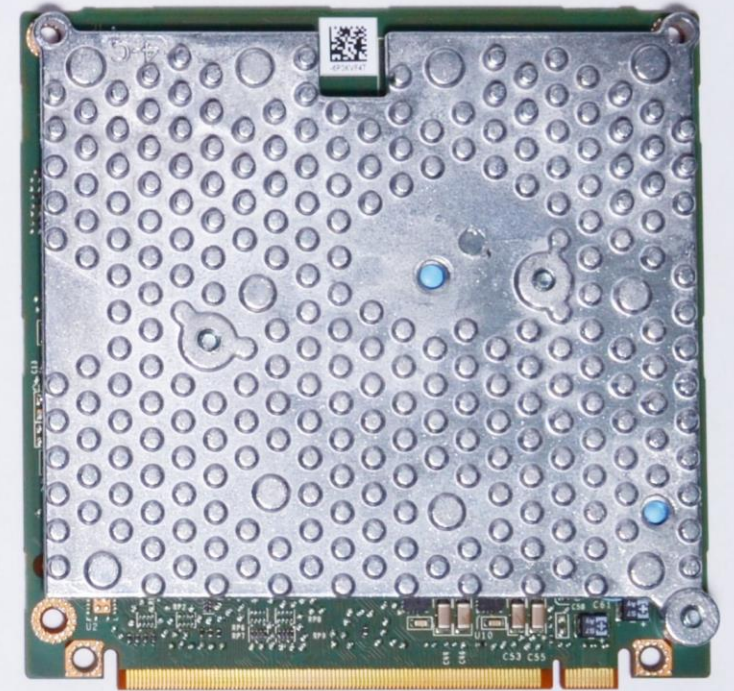
AGRE: FAPL ANRT M-ROD
Número de registro: 192 1056 ANRT 2015
Data de registro: 27/03/2015

CAR 038

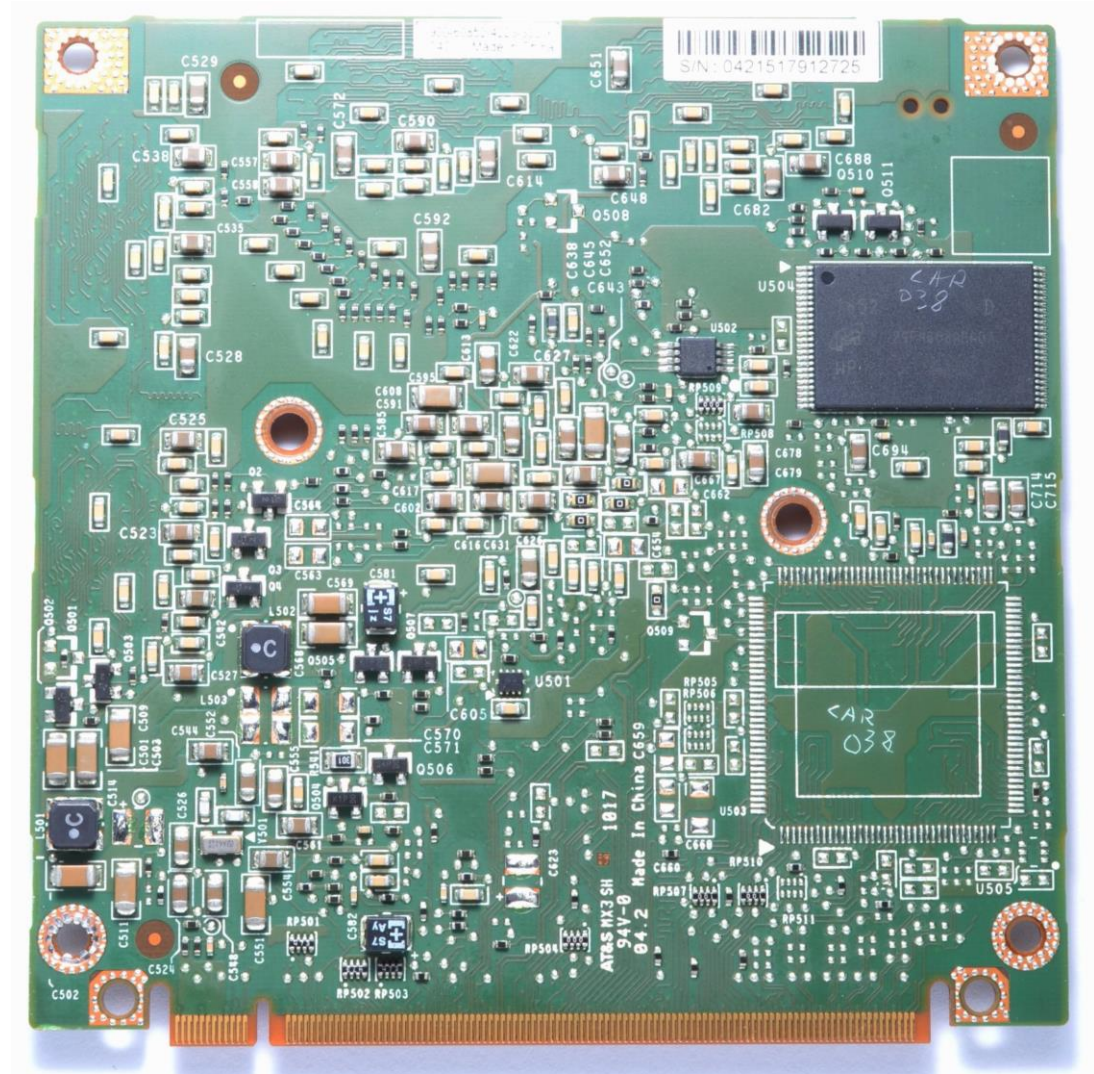
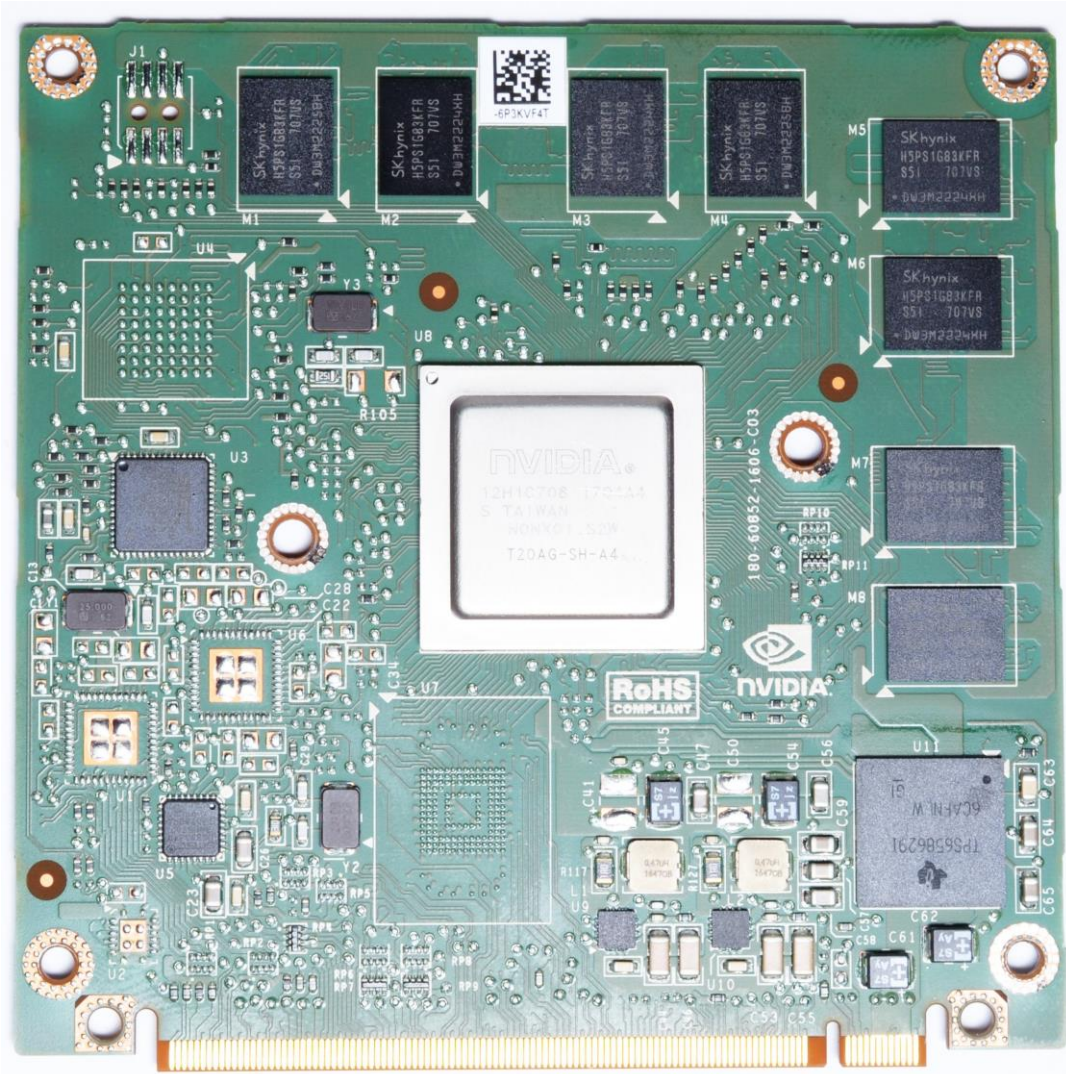
555551173003



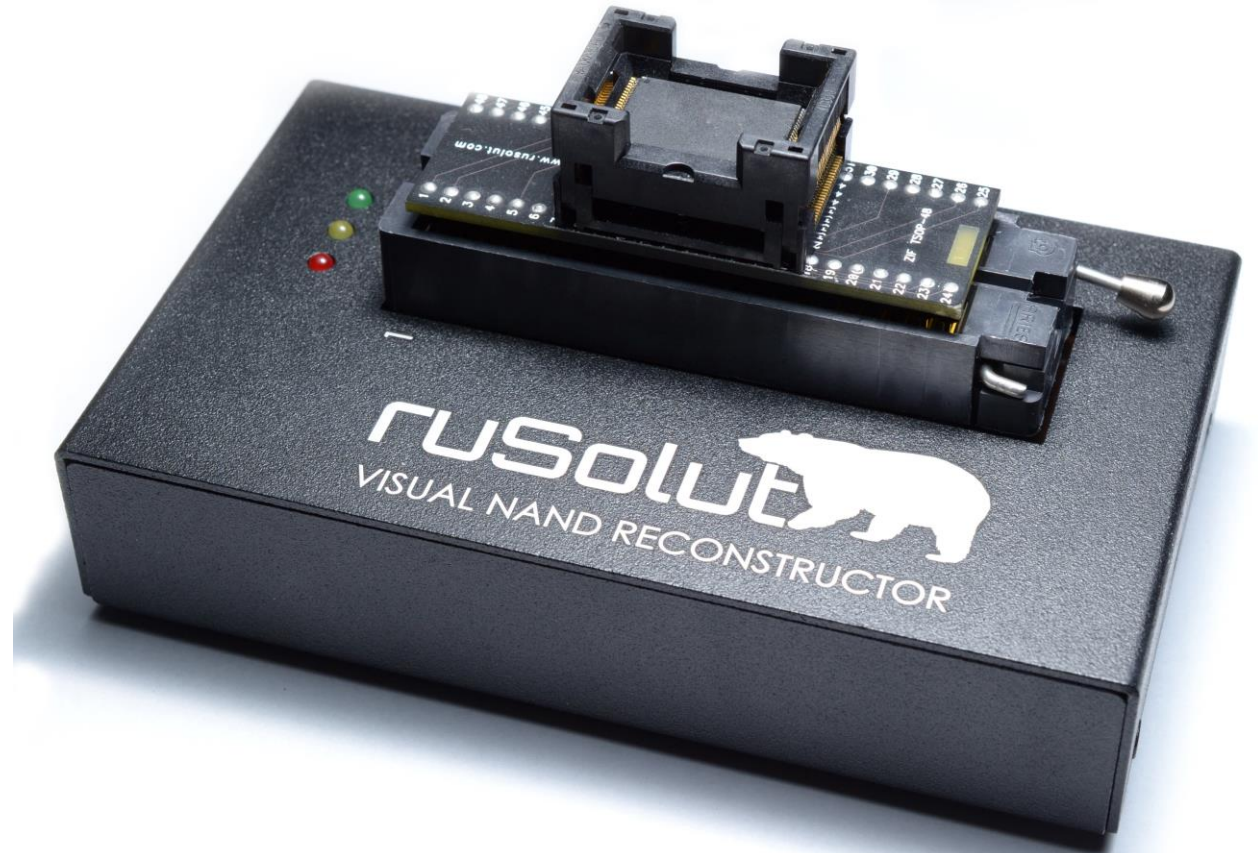
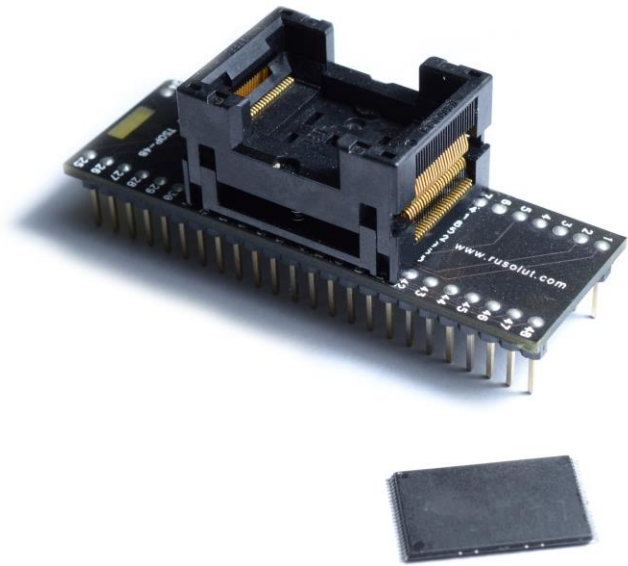
Internal boards



Internal boards



Reading TSOP48...



Case Workspace Plugins Databases

Delete Copy Paste Open images Send solution to Db Insert area Skip area Extract area
 Dump viewer File system viewer Yaffs parser Blocks map File carver File assembler Compute MD5/SHA1 Mount dump Unmount dump Unmount R: drive Find ECC XOR analyzer Codeword analyzer

Element functions Dump functions Dump analysis functio...

Workspace X

Elements Parameters

Enter filter string

Dump operations
 Block list operations
 Other

Reader 0
 Phy image TSOP48
 ECC 0
 Offsets 0
 Data area 0

R Reader PI Physical image
 BCR Bad byte col. remover bBCR Bad bit col. remover
 BCH ECC I Inversion
 X XOR P Pair
 U Unite O Offsets
 LI Logical image
 Hide AI-powered
 X AU XOR X CBM XOR
 X FC XOR X IS XOR
 X ITE XOR X SM XOR
 Hide additional
 SEP Separate ROT Rotate

Element Name 0
 Dump Length (bytes) 553648128
 Automatic structure
 ECC corrector Power Off
 ECC codewords 0 - 511/2052 - 2060/73; 5
 Page size 2112
 Use buffer
 Bytes rotate
 ECC map 0

no errors
 correctable errors
 not correctable errors
 empty

8

Dump adjustment for further parsing

UBI+UBIFS - very popular FS in vehicles and other devices (smarthubs, routers, etc)

ECC 0 X Workspace

Address	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Comment
000FD4D000	55	42	49	23	01	00	00	00	00	00	00	00	00	00	00	00	UBI#.....
000FD4D010	00	00	08	00	00	00	10	00	00	00	10	00	00	00	00	00eA@.....
000FD4D020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00;.+.....
000FD4D030	00	00	00	00	00	00	00	00	00	00	00	00	3B	0C	A2	F7
000FD4D040	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000FD4D050	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000FD4D060	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000FD4D070	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000FD4D080	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000FD4D090	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000FD4D0A0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000FD4D0B0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000FD4D0C0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000FD4D0D0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000FD4D0E0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000FD4D0F0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000FD4D100	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000FD4D110	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000FD4D120	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000FD4D130	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000FD4D140	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000FD4D150	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000FD4D160	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000FD4D170	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000FD4D180	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000FD4D190	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000FD4D1A0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000FD4D1B0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000FD4D1C0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000FD4D1D0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000FD4D1E0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000FD4D1F0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000FD4D200	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000FD4D210	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000FD4D220	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000FD4D230	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000FD4D240	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000FD4D250	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000FD4D260	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000FD4D270	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000FD4D280	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000FD4D290	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000FD4D2A0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000FD4D2B0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000FD4D2C0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000FD4D2D0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000FD4D2E0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000FD4D2F0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000FD4D300	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000FD4D310	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000FD4D320	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000FD4D330	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000FD4D340	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000FD4D350	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF

Byte position: 2070; Row: 125476; Address: 265007382; Value: |

Address: 265605129 Selected: |

No user's data was found here. Only system data on TSOP48

Car Forensics Project - UBI/UBIFS Parser

Open file \\SERVER\fileserver\CONFERENCES\2023_Summit\Conference\Sasha\Car_038\Case\UBI.img

Save selected

ruSolut

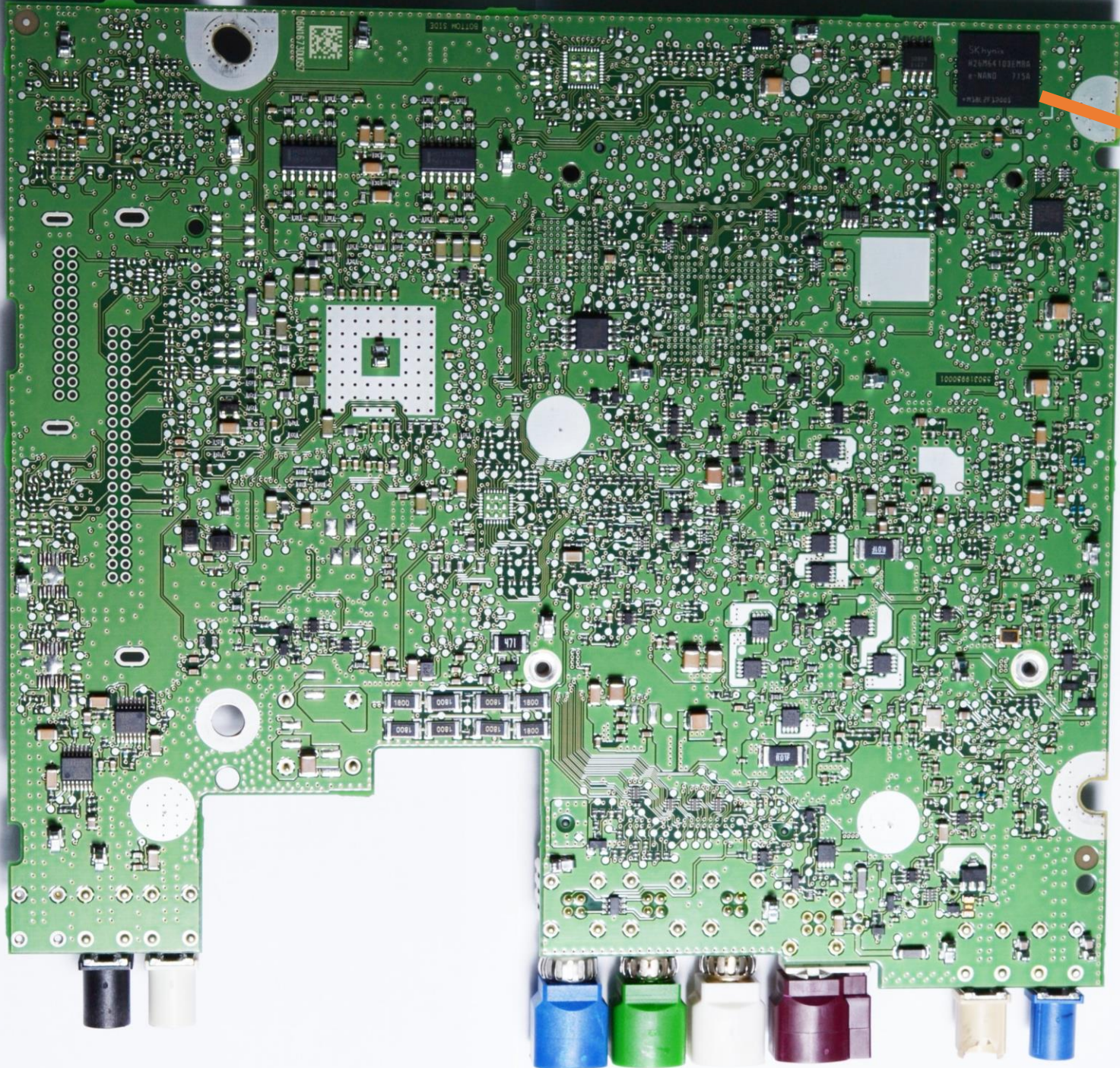
UBI Image Sequence 2135728949

- UBIFS Volume ev_fs
 - Root
 - bin
 - dev
 - etc
 - X11
 - dlt
 - fis
 - lvm
 - msr
 - opt
 - pki
 - ppp
 - rpc
 - ssh
 - xdg
 - nsswitch.conf
 - mounts.xml
 - dlt-system.conf
 - bootwart.conf
 - mtab
 - udev
 - systemd
 - asound.conf.old
 - ld.so.cache
 - lparameters.par
 - iproute2
 - dhclient-udev-script.sh
 - modules-load.d
 - modprobe.d
 - ConsoleKit
 - dhclient.conf
 - default
 - security
 - polkit-1
 - dnsmasq.conf
 - terminfo
 - quotatab

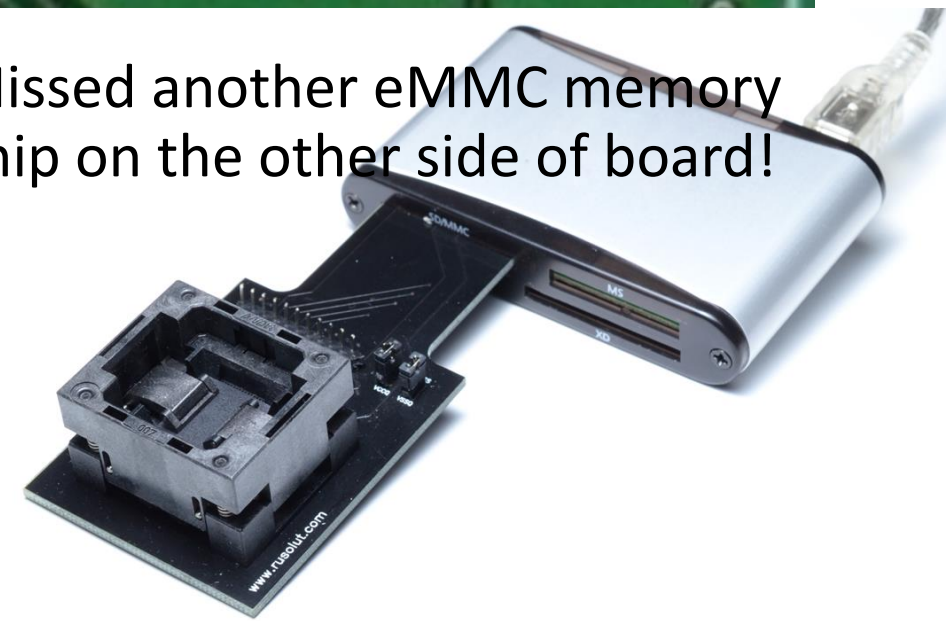
```
Parent inode 65
-> 332 drwxr-xr-x 3 0 0 0 07.02.2019 09:36 X11
-> 304 drwxrwxr-x 2 2009 2009 0 07.02.2019 09:15 dlt
-> 129 drwx----- 4 0 0 0 07.02.2019 09:36 fis
-> 298 drwxr-xr-x 5 0 0 0 07.02.2019 09:36 lvm
-> 80 drwxr-xr-x 2 0 0 0 07.02.2019 09:36 msr
-> 78 drwxr-xr-x 2 0 0 0 07.02.2019 09:05 opt
-> 285 drwxr-xr-x 3 0 0 0 07.02.2019 09:34 pki
-> 83 drwxr-xr-x 2 0 0 0 07.02.2019 09:35 ppp
-> 282 -rwxr-xr-x 1 0 0 1615 17.08.2006 01:18 rpc
-> 103 drwxr-xr-x 2 0 0 0 07.02.2019 09:36 ssh
-> 276 drwxr-xr-x 3 0 0 0 07.02.2019 09:34 xdg
-> 318 -rw-r--r-- 1 0 0 265 07.02.2019 08:47 nsswitch.conf
-> 128 -rw-r--r-- 1 0 0 1818 07.02.2019 09:19 mounts.xml
-> 262 -rw-r--r-- 1 0 0 9702 16.06.2017 14:32 dlt-system.conf
-> 125 -rw-r--r-- 1 0 0 36420 12.09.2017 08:18 bootwart.conf
-> 260 -rwxrwxrwx 1 0 0 0 07.02.2019 09:42 mtab -> /proc/self/
mounts
-> 113 drwxr-xr-x 3 0 0 0 07.02.2019 09:31 udev
-> 338 drwxr-xr-x 2 0 0 0 07.02.2019 09:36 systemd
-> 194 -rw-r--r-- 1 0 0 16944 16.06.2017 14:33 asound.conf.old
-> 100 -rw-r--r-- 1 1000 1000 74532 07.02.2019 09:36 ld.so.cache
```

File iNum	Access	Number of links	UID	GID	Size	Date	Name
332	drwxr-xr-x	3	0	0	0	07.02.2019 09:36	X11
304	drwxrwxr-x	2	2009	2009	0	07.02.2019 09:15	dlt
129	drwx-----	4	0	0	0	07.02.2019 09:36	fis
298	drwxr-xr-x	5	0	0	0	07.02.2019 09:36	lvm
80	drwxr-xr-x	2	0	0	0	07.02.2019 09:36	msr
78	drwxr-xr-x	2	0	0	0	07.02.2019 09:05	opt
285	drwxr-xr-x	3	0	0	0	07.02.2019 09:34	pki
83	drwxr-xr-x	2	0	0	0	07.02.2019 09:35	ppp
282	-rwxr-xr-x	1	0	0	1615	17.08.2006 01:18	rpc
103	drwxr-xr-x	2	0	0	0	07.02.2019 09:36	ssh
276	drwxr-xr-x	3	0	0	0	07.02.2019 09:34	xdg
318	-rw-r--r--	1	0	0	265	07.02.2019 08:47	nsswitch.conf
128	-rw-r--r--	1	0	0	1818	07.02.2019 09:19	mounts.xml
262	-rw-r--r--	1	0	0	9702	16.06.2017 14:32	dlt-system.conf
125	-rw-r--r--	1	0	0	36420	12.09.2017 08:18	bootwart.conf
260	-rwxrwxrwx	1	0	0	0	07.02.2019 09:42	mtab

```
= Address = | ===== HEX file output (up to 1024 bytes) ===== | ===== ASCII =====
-----|-----|-----
0x00000000 | 23 20 64 68 63 70 64 2E 63 6F 6E 66 0A 23 0A 23 | # dhcpd.conf.##
0x00000001 | 20 53 61 6D 70 6C 65 20 63 6F 6E 66 69 67 75 72 | Sample configur
0x00000002 | 61 74 69 6F 6E 20 66 69 6C 65 20 66 6F 72 20 49 | ation file for I
0x00000003 | 53 43 20 64 68 63 70 64 0A 23 0A 0A 23 20 6F 70 | SC dhcpd.## op
0x00000004 | 74 69 6F 6E 20 64 65 66 69 6E 69 74 69 6F 6E 73 | tion definitions
0x00000005 | 20 63 6F 6D 6D 6F 6E 20 74 6F 20 61 6C 6C 20 73 | common to all s
0x00000006 | 75 70 70 6F 72 74 65 64 20 6E 65 74 77 6F 72 6B | upported network
0x00000007 | 73 2E 2E 2E 0A 6F 70 74 69 6F 6E 20 64 6F 6D 61 | s...option doma
0x00000008 | 69 6E 2D 6E 61 6D 65 20 22 65 78 61 6D 70 6C 65 | in-name "example
0x00000009 | 2E 6F 72 67 22 3B 0A 6F 70 74 69 6F 6E 20 64 6F | .org";option do
0x0000000A | 6D 61 69 6E 2D 6E 61 6D 65 2D 73 65 72 76 65 72 | main-name-server
0x0000000B | 73 20 6E 73 31 2E 65 78 61 6D 70 6C 65 2E 6F 72 | s ns1.example.or
0x0000000C | 67 2C 20 6E 73 32 2E 65 78 61 6D 70 6C 65 2E 6F | g, ns2.example.o
0x0000000D | 72 67 3B 0A 0A 64 65 66 61 75 6C 74 2D 6C 65 61 | rg;..default-lea
0x0000000E | 73 65 2D 74 69 6D 65 20 36 30 30 3B 0A 6D 61 78 | se-time 600;max
0x0000000F | 2D 6C 65 61 73 65 2D 74 69 6D 65 20 37 32 30 30 | -lease-time 7200
0x00000010 | 3B 0A 0A 23 20 55 73 65 20 74 68 69 73 20 74 6F | ;..# Use this to
0x00000011 | 20 65 6E 62 6C 65 20 2F 20 64 69 73 61 62 6C 65 | enable / disable
0x00000012 | 20 64 79 6E 61 6D 69 63 20 64 6E 73 20 75 70 64 | dynamic dns upd
0x00000013 | 61 74 65 73 2D 67 6C 6F 62 61 6C 6C 79 2E 0A 23 | ates globally..#
0x00000014 | 64 64 6E 73 2D 75 70 64 61 74 65 2D 73 74 79 6C | dns-update-styl
0x00000015 | 65 20 6E 6F 6E 65 3B 0A 0A 23 20 49 66 20 74 68 | e none;..# If th
0x00000016 | 69 73 20 44 48 43 50 20 73 65 72 76 65 72 20 69 | is DHCP server i
0x00000017 | 73 20 74 68 65 20 6F 66 66 69 63 69 61 6C 20 44 | s the official D
0x00000018 | 48 43 50 20 73 65 72 76 65 72 20 66 6F 72 20 74 | HCP server for t
0x00000019 | 68 65 20 6C 6F 63 61 6C 0A 23 20 6E 65 74 77 6F | he local.# netwo
0x0000001A | 72 6B 2C 20 74 68 65 20 61 75 74 68 6F 72 69 74 | rk, the authorit
0x0000001B | 61 74 69 76 65 20 64 69 72 65 63 74 69 76 65 20 | ative directive
0x0000001C | 73 68 6F 75 6C 64 20 62 65 20 75 6E 63 6F 6D 6D | should be uncomm
0x0000001D | 65 6E 74 65 64 2E 0A 23 61 75 74 68 6F 72 69 74 | ented..#authorit
0x0000001E | 61 74 69 76 65 3B 0A 0A 23 20 55 73 65 20 74 68 | ative;..# Use th
0x0000001F | 69 73 20 74 6F 20 73 65 6E 64 20 64 68 63 70 20 | is to send dhcp
0x00000020 | 6C 6F 67 20 6D 65 73 73 61 67 65 73 20 74 6F 20 | log messages to
0x00000021 | 61 20 64 69 66 66 65 72 65 6E 74 20 6C 6F 67 20 | a different log
0x00000022 | 66 69 6C 65 20 28 79 6F 75 20 61 6C 73 6F 0A 23 | file (you also.#
0x00000023 | 20 68 61 76 65 20 74 6F 20 68 61 63 68 20 73 79 | have to hack sy
0x00000024 | 73 6C 6F 67 2E 63 6F 6E 66 20 74 6F 20 63 6F 6D | slog.conf to com
0x00000025 | 70 6C 65 74 65 20 74 68 65 2D 72 65 64 69 72 65 | plete the redire
0x00000026 | 63 74 69 6F 6E 29 2E 0A 6C 6F 67 2D 66 61 63 69 | ction)..log-faci
0x00000027 | 6C 69 74 79 20 6C 6F 63 61 6C 37 3B 0A 0A 23 20 | lity local7;..#
0x00000028 | 4E 6F 20 73 65 72 76 69 63 65 20 77 69 6C 6C 20 | No service will
0x00000029 | 62 65 20 67 69 76 65 6E 20 6F 6E 20 74 68 69 73 | be given on this
```

Missed another eMMC memory chip on the other side of board!



It was recognized in eMMC adapter, so easy job to read it

The screenshot displays the Visual Nand Reconstructor software interface. The window title is "Visual Nand Reconstructor - Case". The interface is divided into several sections:

- Case:** A tab at the top left.
- File system viewer:** A toolbar with various icons for file system operations such as "Check headers", "Save image", "Save selected", "Check file system", "Create unallocated data dump", "Copy allocated", "Copy unallocated", "Copy selected files data", "Correct allocated", "Correct unallocated", "Correct selected files data", "Android data extractor", "SQLite carver", and "Refresh".
- Workspace:** A central area containing a diagram of the data flow. The diagram shows a sequence of components: "Reader" (0), "Phy image" (TSOP48), "ECC" (0), "Offsets" (0), and "Data area" (0). Below this, there is a section with "eMMC" (0) and "Copy" (0), both marked with red error icons and yellow warning triangles. To the left of the workspace is a vertical toolbar with buttons labeled "R", "PI", "BCR", "bBCR", "BCH", "I", "X", "P", "U", and "O".
- Dump:** A file system tree view on the left side, showing a hierarchy starting with "Dump" and "MBR". It lists several volumes (Volume0 to Volume5) with their respective file systems (EXT-family) and sizes. Volume4 is expanded to show a "Root" directory with subdirectories like "00_integrity", "dtuner", "fis", "hbshare", "HifiTuner", "HifiTuner_evo", "hmi", "lib", "lost+found", "nav", "saf36xxfwloader", and "setup".
- Event log explorer:** A small window at the bottom left.
- Status bar:** At the bottom, it shows "Last active selection: address" and "selected".

Files extracted from file system on eMMC

- %gconf.xml
- 00011A.xml
- A22E75D0D42E059F.bin
- bdaddr.txt
- bmwprovsignedBackUp.xml
- BrowserUrls.db
- bss.bak
- bttempvsdelta.txt
- contactbook
- device_history.list
- develist.dat
- HmiMain3D
- kdz_device_ids.txt
- libnav_ndslib.so
- nav_db.ini
- navpers_NavigationPositioning_Pos_Loc...
- pdl.dat
- pdm_nbt.xml
- pers_NaviControllerLastDestinationsList
- pim01.db
- POIs
- ProvOTABackUpNBT.xml
- service_history.bin
- settings.dat
- sia_device_ids.txt
- statistics_1.dat
- statistics_2.dat
- temp_diag_prov.xml
- timemanager.dat

```
develist.dat
Offset (d) 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15
00000000 01 00 00 00 44 65 76 69 63 65 6C 69 73 74 20 76 ....Devicelist v
00000016 31 2E 30 00 FF FF FF FF FF FF FF FF FF FF FF FF 1.0.YYYYYYYYYYYY
00000032 FF FF FF FF 02 00 00 00 5F 05 63 EB 43 43 3A 32 YYY.Y..._cCC:2
00000048 31 3A 31 39 3A 34 34 3A 36 46 3A 37 45 00 30 30 1:19:44:6F:7E.00
00000064 3A 30 30 3A 30 30 3A 30 30 3A 30 30 3A 30 30 30 :00:00:00:00:00.
00000080 43 43 3A 32 31 3A 31 39 3A 34 34 3A 36 46 3A 37 CC:21:19:44:6F:7
00000096 45 00 30 30 3A 30 30 3A 30 30 3A 30 30 3A 30 30 E.00:00:00:00:00
00000112 3A 30 30 00 43 43 3A 32 31 3A 31 39 3A 34 34 3A :00.CC:21:19:44:
00000128 36 46 3A 37 45 00 47 61 6C 61 78 79 20 41 37 20 6F:7E.Galaxy A7
00000144 28 32 30 31 38 29 00 FF FF FF FF FF FF 47 61 6C 61 (2018).YYYYYGala
00000160 78 79 20 41 37 20 28 32 30 31 38 29 00 FF FF FF xy A7 (2018).YY
00000176 FF FF FF FF 0C 02 5A 00 07 00 00 00 1D 00 00 00 YYY.Y.Z.....
00000192 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000208 00 00 00 00 00 00 00 00 00 00 00 00 00 30 30 3A 30 .....00:0
00000224 30 3A 30 30 3A 30 30 3A 30 30 3A 30 30 00 00 FF 0:00:00:00:00..Y
00000240 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF YYYYYYYYYYYYYYYY
00000256 FF FF FF FF 00 FF FF FF FF FF FF FF FF FF FF FF YYY.YYYYYYYYYYYY
00000272 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF YYYYYYYYYYYY....
00000288 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000304 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000320 00 00 00 00 30 30 3A 30 30 3A 30 30 3A 30 30 3A ....00:00:00:00:
00000336 30 30 3A 30 30 00 00 FF FF FF FF FF FF FF FF FF 00:00..YYYYYYYYYYY
00000352 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF YYYYYYYYYYYYYYYY.YYY
00000368 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF YYYYYYYYYYYYYYYYYYYY
00000384 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 YYY.....
00000400 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000416 00 00 00 00 00 00 00 00 00 00 00 00 30 30 3A 30 .....00:0
00000432 30 3A 30 30 3A 30 30 3A 30 30 3A 30 30 00 00 FF 0:00:00:00:00..Y
00000448 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF YYYYYYYYYYYYYYYYYYYY
00000464 FF FF FF FF 00 FF FF FF FF FF FF FF FF FF FF YYY.YYYYYYYYYYYY
00000480 FF FF FF FF FF FF FF FF FF FF FF FF FF 00 00 00 YYYYYYYYYYYYYYYY....
00000496 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000512 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000528 00 00 00 00 .....

```

```
device_history.list
1
0
0
@END USB_STACK_INFO
##END DEVICE
##START DEVICE 1452:4776 7ac47522bbba266576326633ebf7455deaafa0ad
@START DEVICE_INFO
1
1
0
/dev/hidraw0 /dev/snd/pcmC3D0c
1
512
0
0
0
1452
4776
1794
Apple Inc.
iPhone
7ac47522bbba266576326633ebf7455deaafa0ad
@END DEVICE_INFO
@START USB_STACK_INFO
1452
4776
0
0
4105
4105
4118
4118
1
0
0
@END USB_STACK_INFO
##END DEVICE
##START DEVICE 1452:4776 242fe63b231e4a917ea5c6906e60813dd357d41d
@START DEVICE_INFO
1
1
0
.
```

```
bdaddr.txt
B82410181612
```

Call logs

FD 00 .dat

Offset (d)	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	
00000000	0C	00	00	00	01	00	00	00	00	00	00	00	0C	11	00	00	00	43	43	3A	32	31	3A	31	39	3A	34	34	3A	36	46CC:21:19:46:6F
00000031	3A	37	45	06	00	00	00	CC	21	19	44	6F	7E	01	10	00	00	00	47	61	6C	61	78	79	20	41	37	20	28	30	:7E....i!.Do~....Galaxy A7 (20	
00000062	31	38	29	0F	00	00	00	32	36	30	30	36	30	30	36	38	33	33	38	37	30	36	E2	FF	FF	FF	5A	00	00	00	1E	18)....2600600683...6áyyZ....
00000093	00	00	00	01	BE	F1	FF	FF	42	0E	00	00	3C	00	00	00	01	02	00	00	00	14	00	00	00	00	00	00	00	00	00*áyyB...<.....
00000124	00	00	30	31	2E	30	37	2E	31	39	00	00	00	00	00	0C	00	00	00	2B	34	38	37	33	31	35	34	33	33	33	..01.07.19.....+4873154 333	
00000155	00	00	00	00	05	00	00	00	31	35	3A	35	38	08	00	00	00	31	35	3A	35	38	3A	34	34	01	00	00	00	00	0015:58....15:58:44... ..
00000186	00	00	30	31	2E	30	37	2E	31	39	00	00	00	00	00	0C	00	00	00	2B	34	38	36	30	36	37	35	35	33	33	..01.07.19.....+4860675 333	
00000217	00	00	00	00	05	00	00	00	31	35	3A	34	31	08	00	00	00	31	35	3A	34	31	3A	30	38	00	00	00	00	00	0015:41....15:41:08... ..
00000248	00	00	30	31	2E	30	37	2E	31	39	00	00	00	00	00	0C	00	00	00	2B	34	38	37	32	31	39	39	30	39	38	..01.07.19.....+4872199 998	
00000279	00	00	00	00	05	00	00	00	31	34	3A	32	36	08	00	00	00	31	34	3A	32	36	3A	33	35	00	00	00	00	00	0014:26....14:26:35... ..
00000310	00	00	30	31	2E	30	37	2E	31	39	00	00	00	00	00	0C	00	00	00	2B	34	38	35	31	31	37	31	37	31	31	..01.07.19.....+4851171 191	
00000341	00	00	00	00	05	00	00	00	31	33	3A	31	34	08	00	00	00	31	33	3A	31	34	3A	31	34	00	00	00	00	00	0013:14....13:14:14... ..
00000372	00	00	30	31	2E	30	37	2E	31	39	00	00	00	00	00	0C	00	00	00	2B	34	38	38	38	34	30	32	30	33	34	..01.07.19.....+4888402 304	
00000403	00	00	00	00	05	00	00	00	31	32	3A	35	34	08	00	00	00	31	32	3A	35	34	3A	31	36	01	00	00	00	00	0012:54....12:54:16... ..
00000434	00	00	30	31	2E	30	37	2E	31	39	00	00	00	00	00	0C	00	00	00	2B	34	38	37	33	31	35	34	33	33	33	..01.07.19.....+4873154 333	
00000465	00	00	00	00	05	00	00	00	31	32	3A	30	32	08	00	00	00	31	32	3A	30	32	3A	35	34	01	00	00	00	00	0012:02....12:02:54... ..
00000496	00	00	30	31	2E	30	37	2E	31	39	00	00	00	00	00	0C	00	00	00	2B	34	38	35	31	37	39	31	38	37	39	..01.07.19.....+4851791 749	
00000527	00	00	00	00	05	00	00	00	31	32	3A	30	31	08	00	00	00	31	32	3A	30	31	3A	30	33	00	00	00	00	00	0012:01....12:01:03... ..
00000558	00	00	30	31	2E	30	37	2E	31	39	00	00	00	00	00	0C	00	00	00	2B	34	38	35	31	38	32	35	30	34	30	..01.07.19.....+4851825 470	
00000589	00	00	00	00	05	00	00	00	31	32	3A	30	30	08	00	00	00	31	32	3A	30	30	3A	34	38	00	00	00	00	00	0012:00....12:00:48... ..
00000620	00	00	30	31	2E	30	37	2E	31	39	00	00	00	00	00	0C	00	00	00	2B	34	38	37	33	31	35	34	33	33	33	..01.07.19.....+4873154 333	
00000651	00	00	00	00	05	00	00	00	31	31	3A	35	38	08	00	00	00	31	31	3A	35	38	3A	33	35	00	00	00	00	00	0011:58....11:58:35... ..
00000682	00	00	30	31	2E	30	37	2E	31	39	00	00	00	00	00	0C	00	00	00	2B	34	38	37	33	31	35	34	33	33	33	..01.07.19.....+4873154 333	
00000713	00	00	00	00	05	00	00	00	31	31	3A	35	34	08	00	00	00	31	31	3A	35	34	3A	31	38	00	00	00	00	00	0011:54....11:54:18... ..
00000744	00	00	30	31	2E	30	37	2E	31	39	00	00	00	00	00	0C	00	00	00	2B	34	38	36	39	36	34	35	39	38	35	..01.07.19.....+4869645 845	
00000775	00	00	00	00	05	00	00	00	31	31	3A	31	39	08	00	00	00	31	31	3A	31	39	3A	35	36	01	00	00	00	00	0011:19....11:19:56... ..
00000806	00	00	30	31	2E	30	37	2E	31	39	00	00	00	00	00	0C	00	00	00	2B	34	38	35	33	34	37	37	30	34	34	..01.07.19.....+4853477 444	
00000837	00	00	00	00	05	00	00	00	31	31	3A	30	33	08	00	00	00	31	31	3A	30	33	3A	35	38	00	00	00	00	00	0011:03....11:03:58... ..
00000868	00	00	30	31	2E	30	37	2E	31	39	00	00	00	00	00	0C	00	00	00	2B	34	38	37	32	31	39	39	30	39	38	..01.07.19.....+4872199 998	
00000899	00	00	00	00	05	00	00	00	31	31	3A	30	33	08	00	00	00	31	31	3A	30	33	3A	33	37	00	00	00	00	00	0011:03....11:03:37... ..
00000930	00	00	30	31	2E	30	37	2E	31	39	00	00	00	00	00	0C	00	00	00	2B	34	38	37	39	38	31	37	38	37	37	..01.07.19.....+4879817 757	
00000961	00	00	00	00	05	00	00	00	31	30	3A	33	37	08	00	00	00	31	30	3A	33	37	3A	34	31	01	00	00	00	00	0010:37....10:37:41... ..
00000992	00	00	30	31	2E	30	37	2E	31	39	00	00	00	00	00	0C	00	00	00	2B	34	38	35	30	33	34	35	30	33	35	..01.07.19.....+4850345 355	

Offset: 0

Overwrite

Last destinations

FD AS List

Offset (d)	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31		
00000576	43	41	20	4B	41	4E	54	4F	52	4F	57	49	43	4B	41	00	00	05	01	02	31	38	39	00	00	7C	12	0E	42	08	15	23	CA KANTOROWICKA.....189.. ..B..#	
00000608	A2	19	9B	00	79	15	00	CC	00	00	00	05	00	01	00	A1	00	00	00	03	00	00	00	02	02	01	00	00	00	03	0E	c.>.y..İ.....j.....		
00000640	44	0C	9A	23	A0	F6	1A	00	00	00	00	0E	41	7E	DC	23	9F	6A	FF	00	00	00	00	0E	46	6A	72	23	A2	8C	87	00	D.š# ö.....A~Ü#ÿjÿ.....Fjr#cE#.	
00000672	00	00	00	02	43	3A	50	4F	4C	53	4B	41	7C	54	3A	4B	52	41	4B	C3	93	57	7C	53	3A	55	4C	49	43	41	20	4BC:POLSKA T:KRAKÅ"W S:ULICA K	
00000704	41	4E	54	4F	52	4F	57	49	43	4B	41	7C	48	3A	31	38	39	00	00	00	00	01	00	00	00	00	00	01	0E	42	08	15	ANTOROWICKA H:189.....B..	
00000736	23	A2	19	9B	00	00	00	00	02	00	00	00	00	01	00	05	00	00	00	02	0E	41	7E	DC	23	9F	6A	FF	00	00	00	00	#c.>.....A~Ü#ÿjÿ....	
00000768	0E	46	6A	72	23	A2	8C	87	00	00	00	00	02	00	07	02	00	00	06	00	01	00	00	08	00	01	00	00	09	00	01	00	.Fjr#cE#.....	
00000800	00	0C	00	10	02	70	6F	6C	00	02	50	4F	4C	00	02	4C	61	74	6E	00	02	50	4F	4C	53	4B	41	02	4B	52	41	4Bpol..POL..Latn..POLSKA.KRAK	
00000832	C3	93	57	20	33	31	2D	38	36	38	02	4F	53	49	45	44	4C	45	20	49	49	20	50	55	C5	81	4B	55	20	4C	4F	54	Å"W 31-868.OSIEDLE II PUÅ.KU LOT	
00000864	4E	49	43	5A	45	47	4F	02	02	31	33	02	02	02	02	02	35	39	37	34	34	31	30	31	30	02	32	33	38	37	31	35	NICZEGO..13.....597441010.238715	
00000896	36	37	34	00	00	00	00	07	00	01	01	02	50	4F	4C	53	4B	41	00	00	02	01	02	4B	52	41	4B	C3	93	57	00	00	674.....POLSKA.....KRAKÅ"W..	
00000928	03	01	02	4F	53	49	45	44	4C	45	20	49	49	20	50	55	C5	81	4B	55	20	4C	4F	54	4E	49	43	5A	45	47	4F	00	...OSIEDLE II PUÅ.KU LOTNICZEGO.	
00000960	00	05	01	02	31	33	00	00	7F	01	02	33	31	2D	38	36	38	00	00	7C	12	0E	3A	83	1A	23	9C	39	F2	00	79	1513.....31-868.. ..:f.#œ9ð.y.	
00000992	00	DE	00	00	00	05	00	01	00	B3	00	00	00	03	00	00	00	00	02	02	01	00	00	00	00	03	0E	3A	70	FB	23	9C	3E	.P.....'.....:pû#œ>
0001024	90	00	00	00	00	0E	39	C0	EC	23	9C	12	F1	00	00	00	00	0E	3B	2A	BF	23	9C	8C	FF	00	00	00	00	02	43	3A9Ài#œ.ñ.....;*ç#œÿ.....C:	
0001056	50	4F	4C	53	4B	41	7C	54	3A	4B	52	41	4B	C3	93	57	7C	53	3A	4F	53	49	45	44	4C	45	20	49	49	20	50	55	POLSKA T:KRAKÅ"W S:OSIEDLE II PU	
0001088	C5	81	4B	55	20	4C	4F	54	4E	49	43	5A	45	47	4F	7C	48	3A	31	33	7C	52	3A	33	31	2D	38	36	38	00	00	00	00	Å.KU LOTNICZEGO H:13 R:31-868...
0001120	00	01	00	00	00	00	00	01	0E	3A	83	1A	23	9C	39	F2	00	00	00	00	02	00	00	00	00	01	00	05	00	00	00	02:f.#œ9ð.....	
0001152	0E	39	C0	EC	23	9C	12	F1	00	00	00	00	0E	3B	2A	BF	23	9C	8C	FF	00	00	00	00	02	00	07	02	00	00	06	00	.9Ài#œ.ñ.....;*ç#œÿ.....	
0001184	01	00	00	08	00	01	00	00	09	00	01	00	00	0C	00	10	02	70	6F	6C	00	02	50	4F	4C	00	02	4C	61	74	6E	00pol..POL..Latn..	
0001216	02	50	4F	4C	53	4B	41	02	4B	52	41	4B	C3	93	57	02	55	4C	49	43	41	20	4D	41	53	41	52	53	4B	41	02	02	.POLSKA.KRAKÅ"W.ULICA MASARSKA..	
0001248	02	02	02	02	02	35	39	37	31	38	30	34	31	33	02	32	33	38	30	39	32	36	33	39	00	00	00	00	05	00	01	01597180413.238092639.....	
0001280	02	50	4F	4C	53	4B	41	00	00	02	01	02	4B	52	41	4B	C3	93	57	00	00	03	01	02	55	4C	49	43	41	20	4D	41	.POLSKA.....KRAKÅ"W.....ULICA MA	
0001312	53	41	52	53	4B	41	00	00	7C	12	0E	31	01	5F	23	98	3F	FD	00	79	15	00	CE	00	00	00	05	00	01	00	A3	00	SARSKA.. ..l.#~?ý.y..İ.....£.	
0001344	00	00	03	00	00	00	02	02	01	00	00	00	00	04	0E	31	01	5F	23	98	3F	FD	00	00	00	00	0E	30	8C	DD	23	98l.#~?ý.....0EY#~	
0001376	35	EC	00	00	00	0E	31	5F	DF	23	98	47	8A	00	00	00	0E	31	21	16	23	98	3C	A2	00	00	00	00	02	43			5i.....l_B#~GŠ.....!!.#~<.....C	
0001408	3A	50	4F	4C	53	4B	41	7C	54	3A	4B	52	41	4B	C3	93	57	7C	53	3A	55	4C	49	43	41	20	4D	41	53	41	52	53	:POLSKA T:KRAKÅ"W S:ULICA MASARS	
0001440	4B	41	00	00	00	00	01	00	00	00	00	00	01	0E	31	01	5F	23	98	3F	FD	00	00	00	00	02	00	00	00	00	01	00	KA.....l.#~?ý.....	
0001472	05	00	00	00	02	0E	30	8C	DD	23	98	35	EC	00	00	00	0E	31	5F	DF	23	98	47	8A	00	00	00	00	02	00	05		0EY#~5i.....l_B#~GŠ.....
0001504	02	00	00	06	00	01	00	00	08	00	01	00	00	09	00	01	00	00	0C	00	10	02	70	6F	6C	00	02	50	4F	4C	00	02pol..POL..	
0001536	4C	61	74	6E	00	02	50	4F	4C	53	4B	41	02	57	49	C5	9A	4E	49	C3	93	57	4B	41	20	4D	41	53	C5	81	C3	93	Latn..POLSKA.WIÅSNIÅ"WKA MASÅ.Å"	
0001568	57	02	02	02	02	02	02	02	02	36	30	37	36	39	35	30	33	30	02	32	34	36	36	36	38	39	38	36	00	00	00	00	W.....607695030.246668986....	
0001600	05	00	01	01	02	50	4F	4C	53	4B	41	00	00	02	01	02	57	49	C5	9A	4E	49	C3	93	57	4B	41	00	00	7F	01	02POLSKA.....WIÅSNIÅ"WKA....	
0001632	4D	41	53	C5	81	C3	93	57	00	00	7C	12	0E	B3	DE	BA	24	38	B0	B6	00	79	15	00	A8	00	00	00	05	00	01	00	MASÅ.Å"W.. ..°P°\$8°q.y.."	
0001664	7D	00	00	00	03	00	00	00	02	02	01	00	00	00	00	01	0E	B3	DE	BA	24	38	B0	B6	00	00	00	00	02	43	3A	50	}.....°P°\$8°q.....C:P	
0001696	4F	4C	53	4B	41	7C	54	3A	57	49	C5	9A	4E	49	C3	93	57	4B	41	7C	52	3A	4D	41	53	C5	81	C3	93	57	00	00	OLSKA T:WIÅSNIÅ"WKA R:MASÅ.Å"W..	
0001728	00	00	01	00	00	00	00	00	01	0E	B3	DE	BA	24	38	B0	B6	00	00	00	00	02	00	00	00	00	01	00	05	00	00	00°P°\$8°q.....	

Offset: 0

Overwrite

Phonebook

Visual Nand Reconstructor - Case



Case SQLite carver

Export Remove duplicates Remove unselected

SQLite carver contact_card X Master Table Phy image contactbook_20120928 Workspace

Source
Dump
Template
Search
Start address 0
Run Stop

Carved data
Group by: None Find repeat: CrossSum Simple view

<input type="checkbox"/>	rowid	CrossSum	CrossSumAll	memusage	vcardmemusage	AdditionalName	BMWInfo	GivenName	FamilyName	HowToReadFirstName	HowToReadLastName	Orga
<input checked="" type="checkbox"/>	85	4110468270	1804793804	0	243		0	Ic				
<input checked="" type="checkbox"/>	86	3824486461	331867985	0	264		0	Paulina				
<input checked="" type="checkbox"/>	87	163188078	4086230251	0	256		0	Praca Mama				
<input checked="" type="checkbox"/>	88	4057281176	3031521657	0	264		0	Weglarz				
<input checked="" type="checkbox"/>	89	3537869662	2769572603	0	260		0	Trener Weiss				
<input checked="" type="checkbox"/>	90	3019259467	1741848506	0	248		0	Babcia				
<input checked="" type="checkbox"/>	91	2889359923	1812653437	0	253		0	Konstanty				
<input checked="" type="checkbox"/>	92	3184332993	3616961350	0	249		0	Szmuc				
<input checked="" type="checkbox"/>	93	4213922752	3195527236	0	246		0	Hugo				
<input checked="" type="checkbox"/>	94	2285617048	2006296946	0	245		0	Ola				
<input checked="" type="checkbox"/>	95	836665506	436116718	0	313		0	Fabian Służbowy				
<input checked="" type="checkbox"/>	96	1050274559	1574013353	0	246		0	Lucas				
<input checked="" type="checkbox"/>	97	3006237490	3187954933	0	253		0	Samsung				
<input checked="" type="checkbox"/>	98	1053319548	1543015028	0	263		0	Famat				
<input checked="" type="checkbox"/>	99	1948025434	3252539309	0	251		0	Kurier				
<input checked="" type="checkbox"/>	100	1706579541	1732902687	0	263		0	Bozena				



Export

Remove
duplicatesRemove
unselected

Phonebook

SQLite carver phone_data_phone X Master Table Phy image contactbook_20120928 Workspace

Source

Dump

Template

Search

Start address

Carved data

Group by: None

<input type="checkbox"/>	rowid	Contact_ID	PhoneIndex	CrossSum	PhoneType	PhoneNumber	NormalizedNumber	Position	Algorithm	Encoding
<input checked="" type="checkbox"/>	1	0	0	0	3341		0	24552	N1 N2 N3 N4 N5 S6 N7	
<input checked="" type="checkbox"/>	1	2	0	0	3	575241	75241	5	237545	N1 N2 N3 N4 N5 S6 N7
<input checked="" type="checkbox"/>	2	3	0	0	3	+48501569	1569	7	237518	N1 N2 N3 N4 N5 S6 N7
<input checked="" type="checkbox"/>	3	4	0	0	3	+48501968	1968	4	237491	N1 N2 N3 N4 N5 S6 N7
<input checked="" type="checkbox"/>	4	5	0	0	3	+48602713	2713	9	237464	N1 N2 N3 N4 N5 S6 N7
<input checked="" type="checkbox"/>	5	6	0	0	3	+48601586	1586	8	237437	N1 N2 N3 N4 N5 S6 N7
<input checked="" type="checkbox"/>	6	7	0	0	3	1111	11	11	237419	N1 N2 N3 N4 N5 S6 N7
<input checked="" type="checkbox"/>	7	8	0	0	3	+487988	988	988729	237391	N1 N2 N3 N4 N5 S6 N7
<input checked="" type="checkbox"/>	8	9	0	0	3	692051	92051	9	237366	N1 N2 N3 N4 N5 S6 N7
<input checked="" type="checkbox"/>	9	10	0	0	3	+485311	31168	9	237338	N1 N2 N3 N4 N5 S6 N7
<input checked="" type="checkbox"/>	10	11	0	0	3	+48517918	17918	9	237310	N1 N2 N3 N4 N5 S6 N7
<input checked="" type="checkbox"/>	11	12	0	0	3	+4850675	675	0	237283	N1 N2 N3 N4 N5 S6 N7
<input checked="" type="checkbox"/>	12	13	0	0	3	509089	9089	7	237258	N1 N2 N3 N4 N5 S6 N7
<input checked="" type="checkbox"/>	13	14	0	0	3	601777	1777	9	237234	N1 N2 N3 N4 N5 S6 N7
<input checked="" type="checkbox"/>	14	15	0	0	3	+487940	94041	2	237206	N1 N2 N3 N4 N5 S6 N7
<input checked="" type="checkbox"/>	15	16	0	0	3	+4888555	8555	7	237178	N1 N2 N3 N4 N5 S6 N7
<input checked="" type="checkbox"/>	16	17	0	0	3	+4850290	2906	4	237151	N1 N2 N3 N4 N5 S6 N7
<input checked="" type="checkbox"/>	17	18	0	0	3	+4884627	4627	30	237123	N1 N2 N3 N4 N5 S6 N7
<input checked="" type="checkbox"/>	18	19	0	0	3	5035211	35211	44	237099	N1 N2 N3 N4 N5 S6 N7
<input checked="" type="checkbox"/>	19	20	0	0	3	660047	60047	51	237074	N1 N2 N3 N4 N5 S6 N7
<input checked="" type="checkbox"/>	20	21	0	0	3	+48515	1530	69	237046	N1 N2 N3 N4 N5 S6 N7
<input checked="" type="checkbox"/>	21	22	0	0	3	+486964	9645	45	237018	N1 N2 N3 N4 N5 S6 N7
<input checked="" type="checkbox"/>	22	23	0	0	3	783959	8395	38	236993	N1 N2 N3 N4 N5 S6 N7

Position 1 from 660

Citroen C3 Aircross (real case)

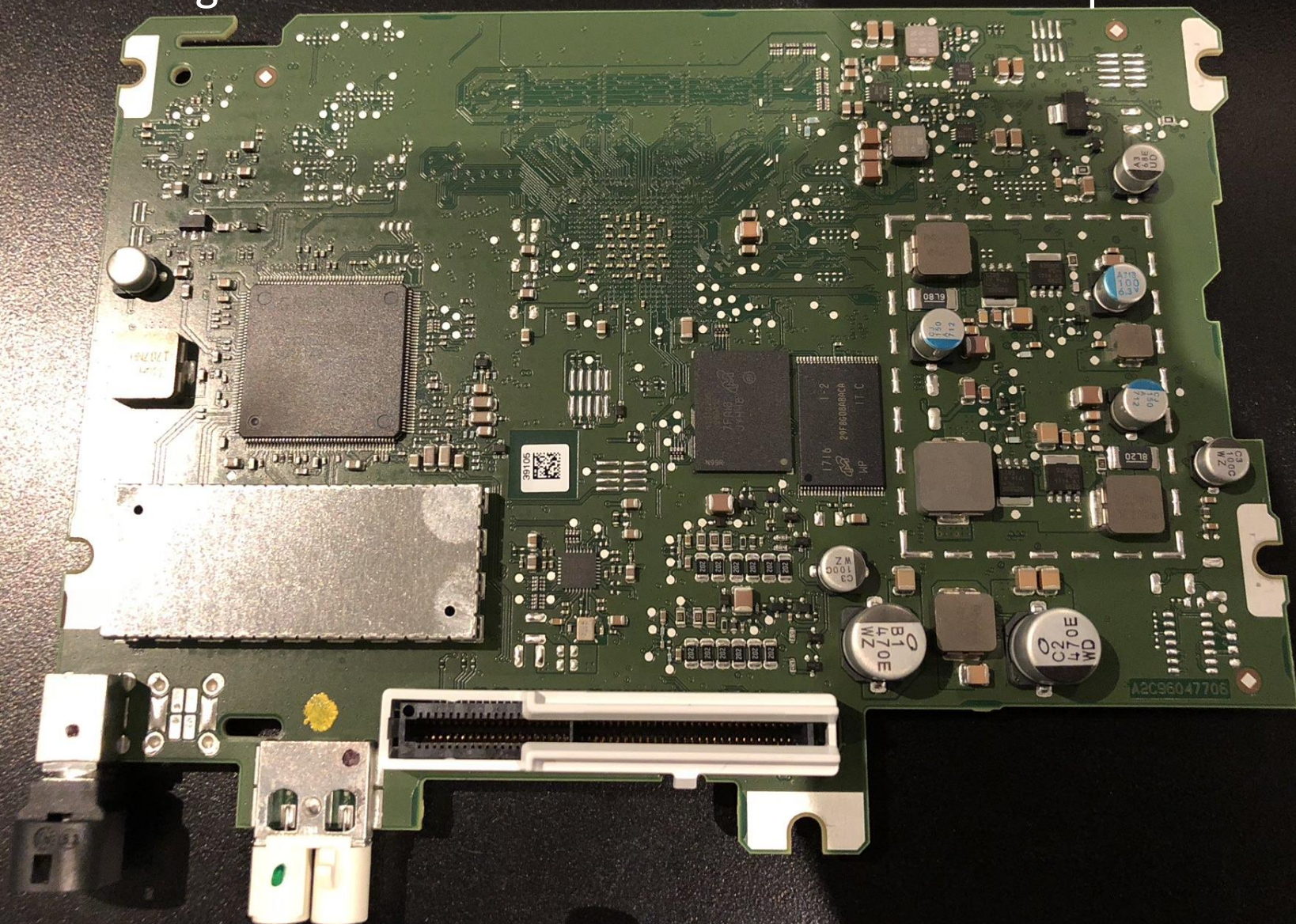




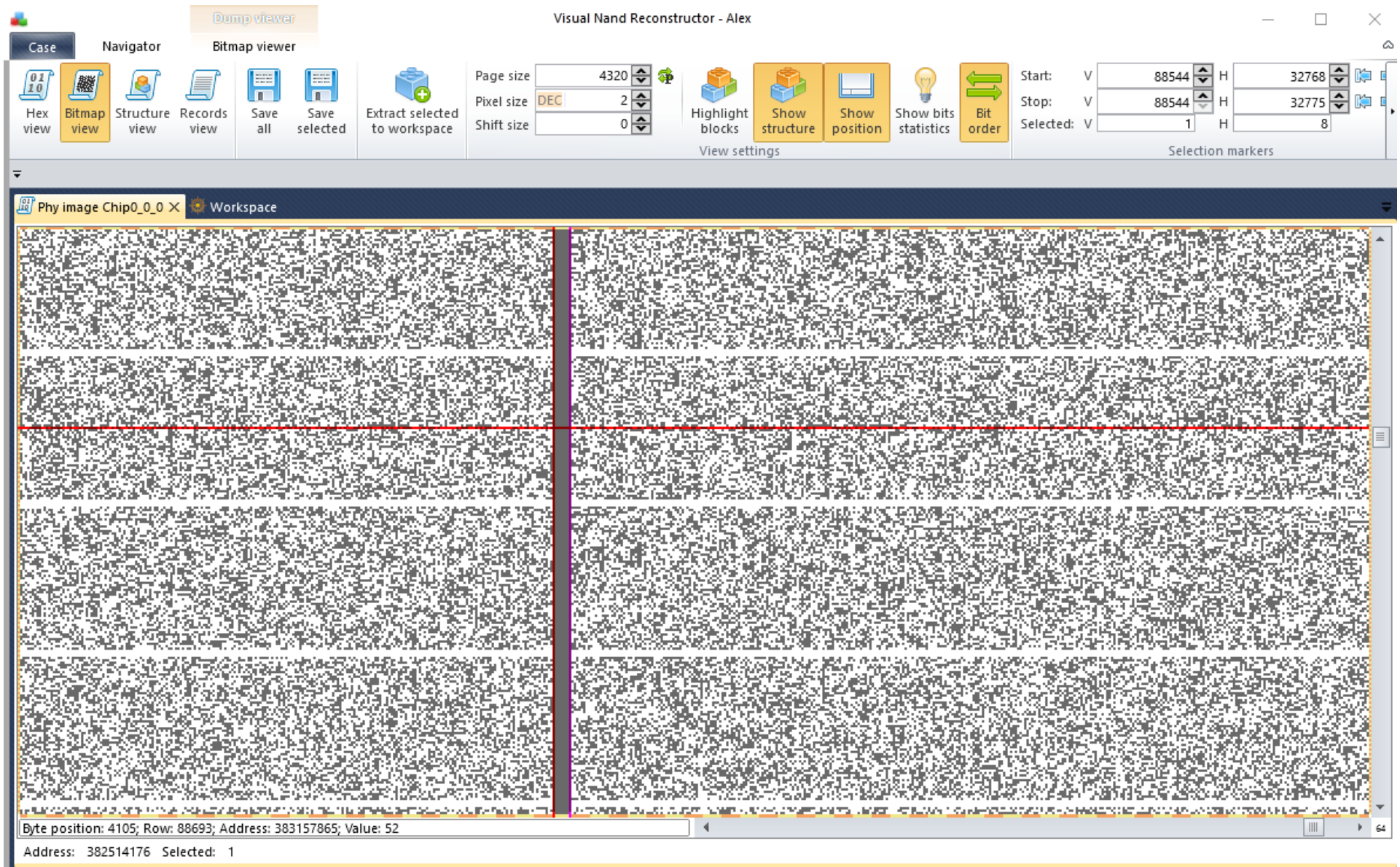
Great view!



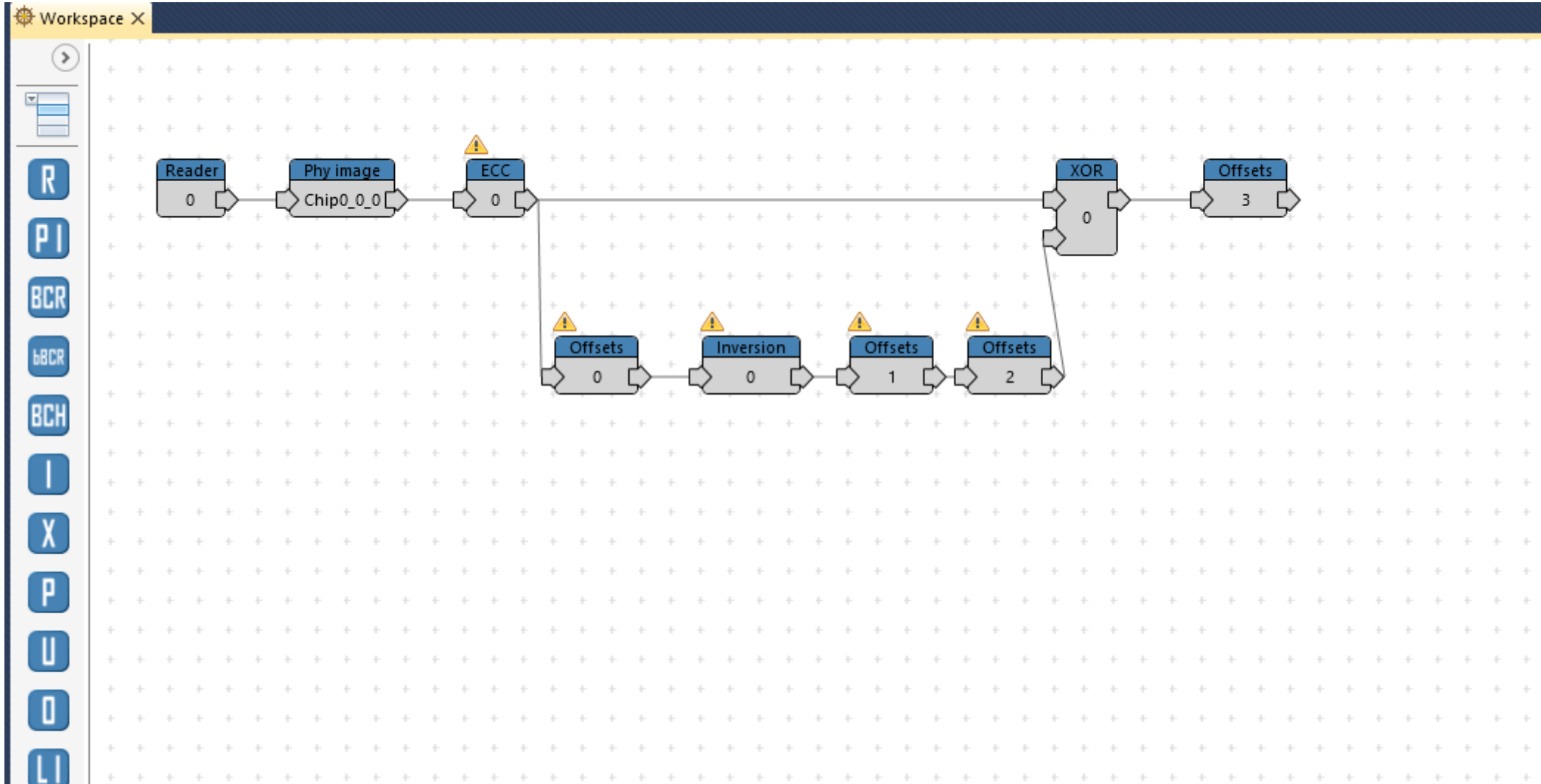
We only got a dumps from the case.
It was Continental NAC_EUR_WAVE2 computer.
Single 1GB Micron 29F8G08ABACA TSOP48 chip.



The page layout was unusual with some data bytes shifted and dummy bytes inserted



Page structure had to be adjusted right after ECC correction



UBIFS again!

Visual Nand Reconstructor - Alex

Case Navigator Hex viewer Bitmap viewer

Hex view Bitmap view Structure view Records view Save all Save selected Extract selected to workspace Frame view Show structure

Frame size: 4320
Current frame: 59648 / 262143

View settings

Offsets 3 X Workspace

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
000F5BE000	55	42	49	23	01	00	00	00	00	00	00	00	00	00	00	02	UBI#.....
000F5BE010	00	00	10	00	00	00	20	00	EC	ED	F6	62	00	00	00	00iïöb....
000F5BE020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000F5BE030	00	00	00	00	00	00	00	00	00	00	00	00	BF	DD	D7	F7çÿ×+
000F5BE040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000F5BE050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000F5BE060	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000F5BE070	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000F5BE080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000F5BE090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000F5BE0A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000F5BE0B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000F5BE0C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000F5BE0D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000F5BE0E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000F5BE0F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000F5BE100	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000F5BE110	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000F5BE120	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000F5BE130	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000F5BE140	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000F5BE150	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000F5BE160	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000F5BE170	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000F5BE180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000F5BE190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000F5BE1A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000F5BE1B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000F5BE1C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000F5BE1D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000F5BE1E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000F5BE1F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000F5BE200	BD	9A	90	5C	01	ED	3D	EF	A4	7E	66	13	D7	9A	BA	DD	¸g[]\,i=iR~f.×š°ÿ
000F5BE210	F2	54	A8	A8	A8	6F	0B	92	24	1F	00	00	00	00	00	00	øT""o.'\$.....
000F5BE220	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000F5BE230	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

Byte position: 28; Row: 59559; Address: 2572

Address: 257679364 Selected:

This time we got an interesting set of data out of UBIFS

ApplicationTimeStamp.dat	19/12/2018 3:07 pm
Home.dat	21/03/2018 5:54 pm
LastDestination.db	19/12/2018 3:07 pm
LastRoute.dat	10/10/2018 2:55 am
POICategoryFilterMapView.dat	19/12/2018 3:04 pm
POICategoryFilterSearch.dat	18/05/2015 5:25 pm
PreferredAddress.db	18/05/2015 5:25 pm
Work.dat	15/09/2018 4:50 pm

Table: NavigableLocation

	id	address
	Filter	Filter
1	1	BLOB
2	2	BLOB
3	3	BLOB
4	4	BLOB
5	5	BLOB
6	6	BLOB
7	7	BLOB
8	8	BLOB
9	9	BLOB
10	10	BLOB
11	11	BLOB
12	12	BLOB
13	13	BLOB

Go to: 1

Mode: Binary

Import Export Set as NULL

0000 00 00 00 10 00 43 00 41 00 64 00 64 00 72 00 65 C. A. d. d. r. e
0010 00 73 00 73 00 00 00 1c 00 55 00 6e 00 69 00 74	. s. s. U. n. i. t
0020 00 65 00 64 00 20 00 4b 00 69 00 6e 00 67 00 64	. e. d. . K. i. n. g. d
0030 00 6f 00 6d 00 00 00 06 00 47 00 42 00 52 00 00	. o. n. G. B. R. .
0040 00 0e 00 42 00 65 00 6c 00 66 00 61 00 73 00 74	... B. e. l. f. a. s. t
0050 00 00 00 1a 00 4d 00 79 00 20 00 4c 00 61 00 64 M. y. . L. a. d
0060 00 79 00 73 00 20 00 52 00 6f 00 61 00 64 ff ff	. y. s. . R. o. a. d. .
0070 ff ff 00 00 00 02 00 32 ff ff ff ff ff ff ff ff 2.
0080 00 00 00 06 00 42 00 54 00 36 00 00 00 0e 00 42 B. T. 6. B
0090 00 65 00 6c 00 66 00 61 00 73 00 74 00 00 00 00	. e. l. f. a. s. t.
00a0 00 00 00 00 40 4b 4b c1 69 c2 3b 79 c0 17 a4 28 @KK. i. ; y. ... (
00b0 4d fc e3 15 01 ff ff ff ff ff ff ff ff 01	M.

Type of data currently in cell: Binary
190 byte(s)

Apply

my ladys road 2

2 My Ladys Rd

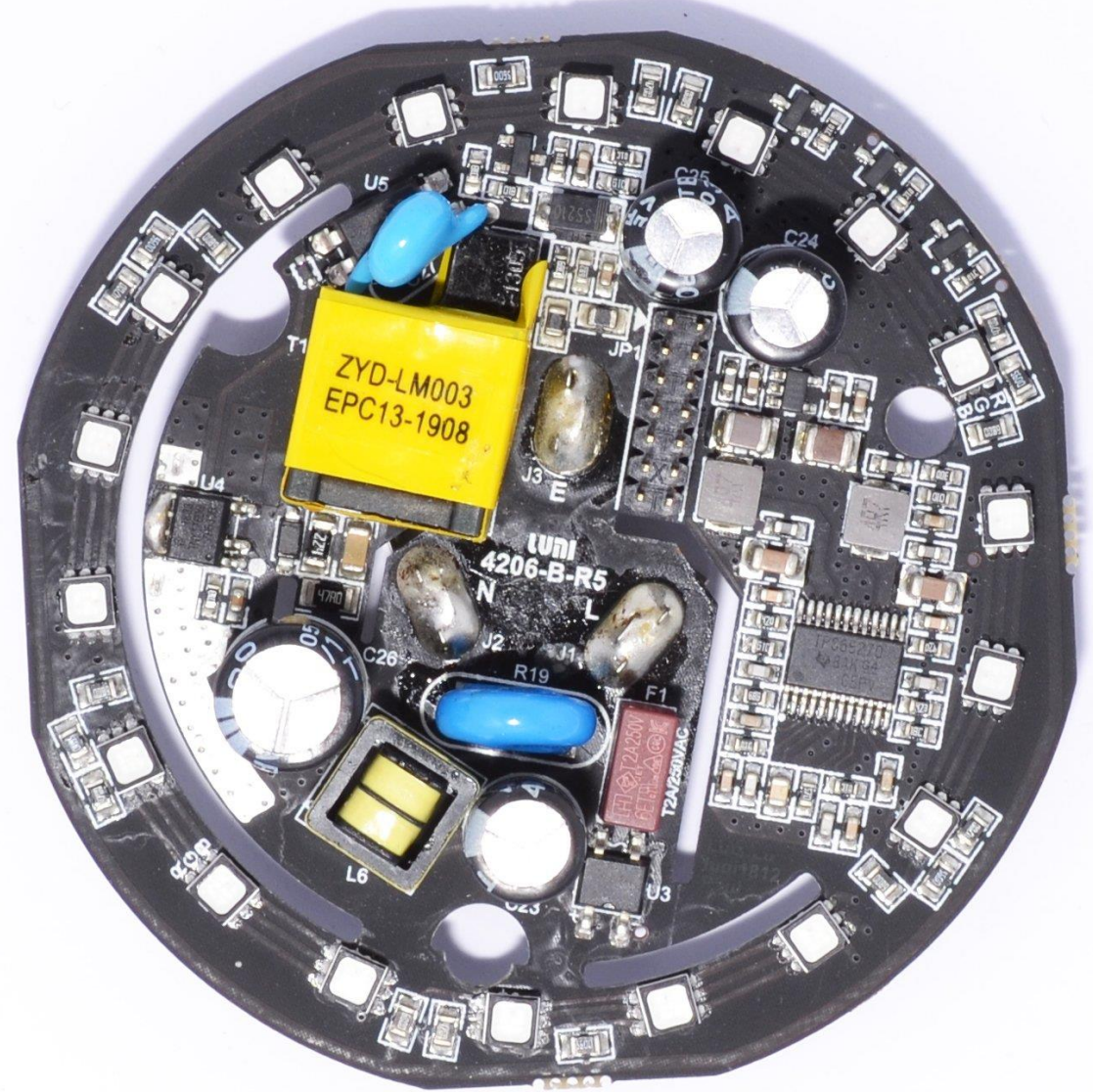
[Wyznacz trasę](#)
[Zapisz](#)
[W pobliżu](#)
[Wyślij na telefon](#)
[Udostępni](#)

[2 My Ladys Rd, Belfast BT6 8HU, Wielka Brytania](#)
[Potwierdź lub popraw tę lokalizację](#)
 Wyświetlona lokalizacja jest niedokładna
[Zaproponuj zmianę dotyczącą: 2 My Ladys Rd](#)
[Dodaj brakujące miejsce](#)
[Dodaj swoją firmę](#)
[Dodaj etykietę](#)

Xiaomi smart home gateway/hub V2 DGNWG05LM (sacrificed own hub in the name of science)



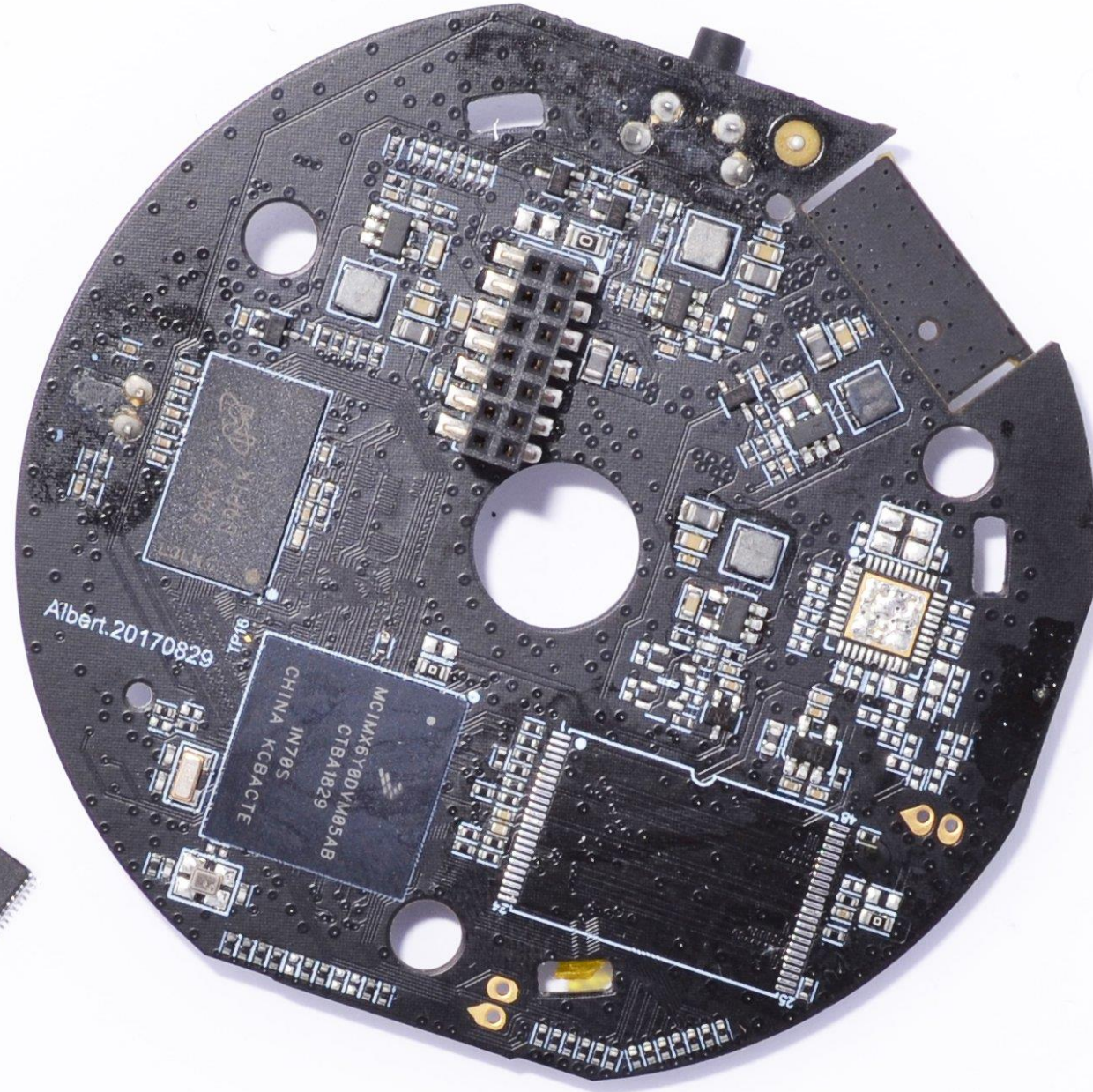
Analog PCB (power management, pwm led controller, leds, etc)



Digital PCB (ZigBee, Wi-Fi modules)



Digital PCB (MCU, NAND, RAM)



TSOP48 NAND

A bit of transformations of physical image...as always

The screenshot displays the Visual NAND Reconstructor interface for a Xiaomi V2 device. The main workspace shows a workflow diagram for processing a physical NAND image:

- Reader** (0) → **Phy image** (Chip0_0_0) → **ECC** (0)
- The **ECC** block branches into three **Offsets** blocks:
 - 1 byte
 - 2038 bytes
 - 35 bytes
- These three **Offsets** blocks feed into a **Concatenate** block (0).
- The **Concatenate** block feeds into an **Offsets** block (0).
- The final **Offsets** block feeds into a **Copy** block (0).


The interface includes a top menu bar with 'Case', 'Workspace', 'Plugins', and 'Databases'. A toolbar contains 'Delete', 'Copy', 'Paste', 'Open images', and 'Send solution to Db'. A 'Solution' panel on the right shows device details: Controller (2CDA909506), Memory chip ID, Number of memory chips (1), and Number of crystals (1). A 'Premium Support' banner is also visible.

File system is “slightly” corrupted (or just another modification of UBIFS...research required)

Car Forensics Project - UBI/UBIFS Parser

Open file: \\SERVER\fileserver\R&D\IOT\SmartHubs\XiaomiV2_DGNWG05LM_SashaHome\UBI.bin

Save selected

ruSolut 

▲ UBI Image Sequence 181309907
 ▲ UBIFS Volume rootfs
 Root

```

-> 65      drwxrwxrwx  2    1028  1035  0    01.01.1970 00:06 bin
-> 206     drwxrwxrwx  2    1028  1035  0    28.07.2018 02:10 dev
-> 207     drwxrwxrwx  49   1028  1035  0    09.09.2022 05:07 etc
-> 1240    Lost inode of file
-> 1547    Lost inode of file
-> 1549    Lost inode of file
-> 1690    Lost inode of file
-> 1846    Lost inode of file
-> 1845    Lost inode of file
-> 5776    Lost inode of file
-> 1848    Lost inode of file
-> 5815    Lost inode of file
-> 205     drwxrwxrwx  2    1028  1035  0    28.07.2018 02:10 boot
-> 886     Lost inode of file
-> 1493    Lost inode of file
-> 1689    Lost inode of file
-> 1691    Lost inode of file
-> 1546    Lost inode of file
-> 5836    Lost inode of file
  
```

File iNum	Access	Number of links	UID	GID	Size	Date	Name
65	drwxrwxrwx	2	1028	1035	0	01.01.1970 00:06	bin
206	drwxrwxrwx	2	1028	1035	0	28.07.2018 02:10	dev
207	drwxrwxrwx	49	1028	1035	0	09.09.2022 05:07	etc
0		0	0	0	0		Lost inode of file lib
0		0	0	0	0		Lost inode of file mnt
0		0	0	0	0		Lost inode of file opt
0		0	0	0	0		Lost inode of file run
0		0	0	0	0		Lost inode of file tmp
0		0	0	0	0		Lost inode of file sys
0		0	0	0	0		Lost inode of file var
0		0	0	0	0		Lost inode of file usr
0		0	0	0	0		Lost inode of file wpa
205	drwxrwxrwx	2	1028	1035	0	28.07.2018 02:10	boot
0		0	0	0	0		Lost inode of file home
0		0	0	0	0		Lost inode of file lumi
0		0	0	0	0		Lost inode of file proc

Quick Hex analysis reveals the WiFi SSID and password in plain text :D

Copy 0 X Workspace

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
0010210010	2D	39	6C	1E	05	20	0A	09	65	78	65	63	20	2A	78	01	-91.. ..exec *x.
0010210020	09	77	20	26	20	20	0A	66	69	20	20	0A	0A	11	00	00	.w & .fi
0010210030	31	18	10	06	A4	02	D8	7A	0B	46	08	00	00	00	00	00	1...x.0z.F.....
0010210040	C8	00	00	00	01	00	00	00	49	02	00	00	00	00	00	20	È.....I.....
0010210050	00	00	00	00	00	00	00	00	98	00	00	00	00	00	00	00~.....
0010210060	63	74	72	6C	5F	69	6E	74	65	72	66	61	63	65	3D	2F	ctrl_interface=/
0010210070	76	61	72	2F	72	75	6E	2F	77	70	61	5F	73	75	70	70	var/run/wpa_supp
0010210080	6C	69	63	61	6E	74	0A	75	70	64	61	74	65	5F	63	6F	licant.update_co
0010210090	6E	66	69	67	3D	31	0A	0A	6E	65	74	77	6F	72	6B	3D	nfig=1..network=
00102100A0	7B	0A	09	73	73	69	64	3D	22	58	69	61	6F	6D	69	5F	{..ssid="XiaoMi_
00102100B0	32	42	34	42	22	0A	09	73	63	61	6E	5F	73	73	69	64	2B4B"..scan_ssid
00102100C0	3D	31	0A	09	70	73	6B	3D	22	36	34	32	47	74	36	32	=1..psk="6
00102100D0	21	36	22	0A	09	6B	65	79	5F	6D	67	6D	74	3D	57	50	="..key_mgmt=WP
00102100E0	41	2D	50	53	4B	0A	09	70	72	6F	74	6F	3D	57	50	41	A-PSK..proto=WPA
00102100F0	20	57	50	41	32	0A	7D	0A	31	18	10	06	83	5C	EB	BF	WPA2.}.1...f\è;
0010210100	09	43	D7	C5	72	31	DE	60	84	00	00	00	00	00	70	3D	.CxArlP`.....p=
0010210110	00	00	10	00	00	00	90	7E	01	00	00	00	00	00	02	00~.....
0010210120	00	00	00	00	00	00	90	6A	00	00	10	00	00	00	00	50~j.....P
0010210130	B0	27	02	23	A2	23	12	C6	16	26	D7	F6	15	E3	D2	06	°'.#o#.E.&xö.ãÖ.
0010210140	37	23	C2	22	12	23	A2	53	2C	20	43	2E	A0	00	23	A2	7#Ã".#oS, C. #o
0010210150	23	42	F6	F6	26	F7	25	56	C6	C6	86	02	0A	40	56	80	#Böö&+§VEE+..@VE
0010210160	82	05	70	52	0B	20	B3	52	0B	30	13	8F	30	B3	92	05	..pR. 'R.O.0'.
0010210170	40	83	2D	00	57	C0	FB	10	5E	20	43	D7	40	70	57	C6	@f-.WÀû.^ Cx@pWE
0010210180	36	F6	D6	56	76	D2	1A	20	C3	D6	00	2F	50	DE	20	03	6öÖVvò. ÄÖ./PB .
0010210190	77	00	2F	70	82	0F	C0	C7	00	2F	70	42	19	10	40	23	w./p,.ÄÇ./pB..@#
00102101A0	A2	23	12	2F	50	93	FE	50	93	12	05	60	13	2F	60	93	o#./P"bP"..../"
00102101B0	12	05	70	13	2F	70	93	12	05	80	13	2F	80	93	12	05	..p./p"..è./è"..
00102101C0	90	13	2F	90	93	22	05	10	03	43	2D	80	26	01	CB	01	□./□"...C-è.&.È.
00102101D0	2E	C1	17	41	2A	40	1F	01	17	41	2A	80	1E	41	16	41	.Ä.A*@...A*è.A.A
00102101E0	2A	C0	0F	81	07	41	2A	00	0F	C1	06	41	2A	40	0E	41	*Ä.□.A*...Ä.A*@.A
00102101F0	1B	90	30	47	17	46	57	37	27	A2	23	02	23	C2	42	9D	.□OG.FW7'°#. #ÄB□
0010210200	93	40	97	D6	56	F6	C5	56	E6	26	A2	23	32	83	42	05	"@-ÖVöAVæ&o#2fB.
0010210210	60	60	17	C6	56	57	26	A2	23	22	73	C2	09	20	60	F7	`.EVW&o#"sÄ.÷
0010210220	C6	56	D7	86	26	00	49	30	20	D7	96	E6	76	F6	C5	82	EVx†&.IO x-ævöÄ,
0010210230	13	C0	2A	C0	99	60	40	56	C6	16	96	27	A2	23	62	93	.Ä*AÄ"@VE.-'o#b"
0010210240	02	0B	80	AE	60	10	53	83	93	23	03	03	73	03	43	A7	..è@`.Sf"#.s.CS
0010210250	74	30	86	96	06	67	55	26	37	97	F6	06	06	A1	20	E3	t0+-.gU&7-ö..; ä
0010210260	22	43	23	C2	22	32	C6	F6	36	B6	F6	D5	5F	20	C3	86	"C#Ä"2Eö6qöÖ_ Ä†

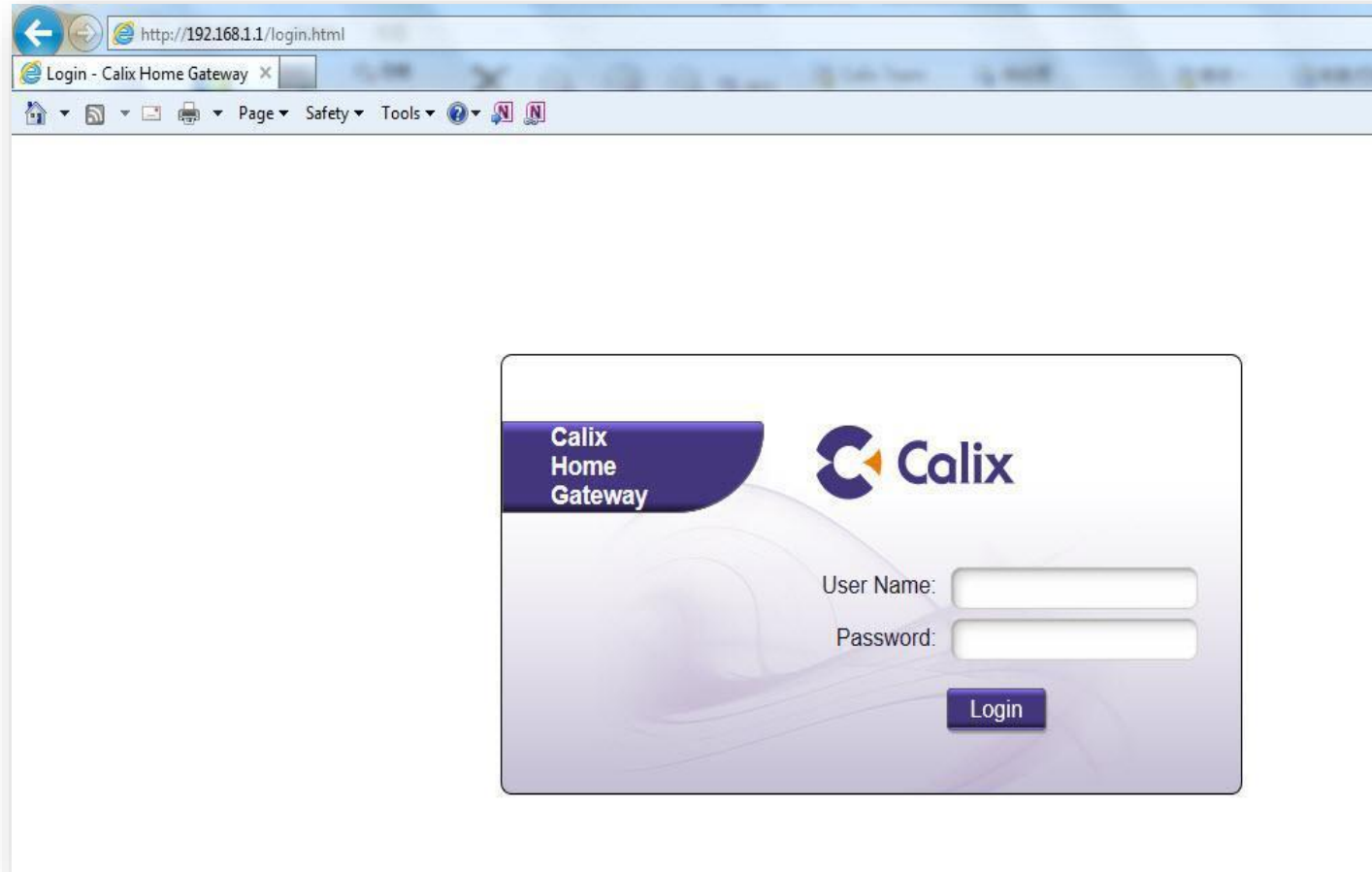
Byte position: 34; Row: 128188; Address: 2707330E

Address: 270597918 Selected: 0

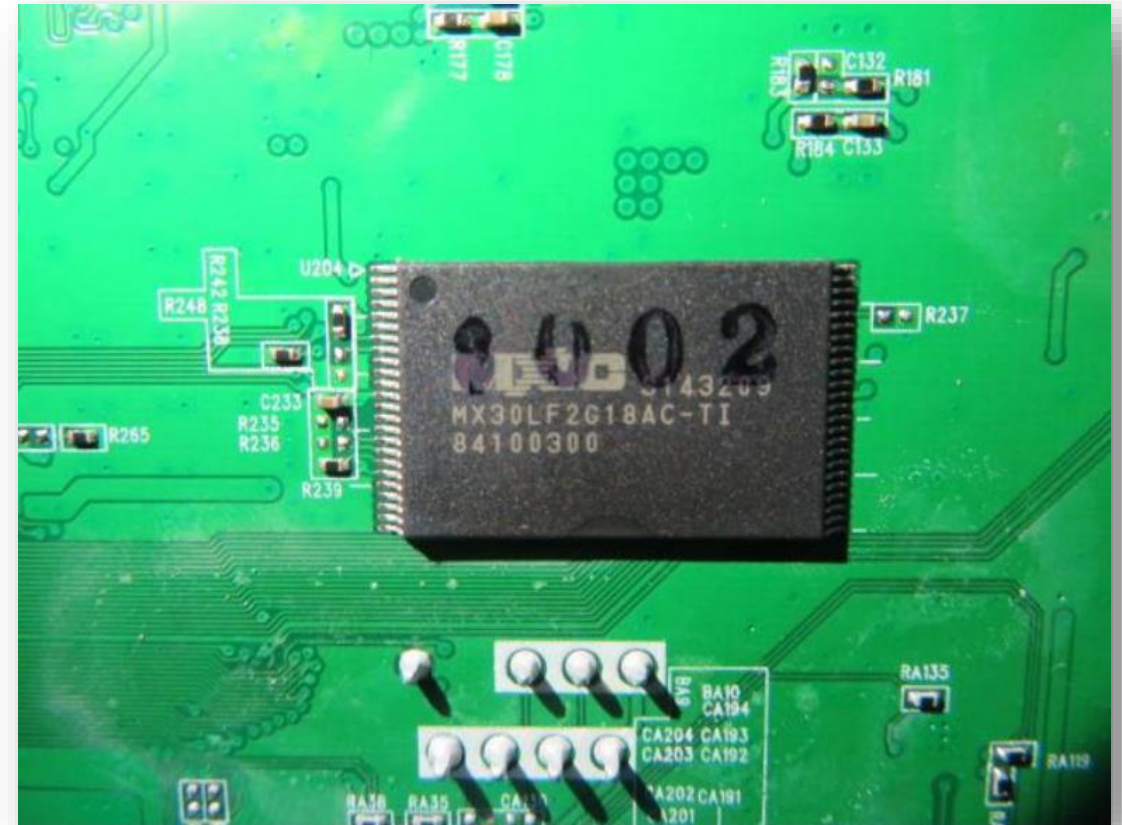
Router CALIX 844E-1 (real case)



Web access – no password (seized device)



Board and chip (TSOP48)



NAND reading

The screenshot shows the Visual NAND Reader software interface. At the top, there are tabs for 'Case', 'Workspace', and 'Plugins'. Below these is a toolbar with icons for 'Delete', 'Copy', 'Open images', 'Insert area', 'Skip area', 'Extract area', 'Remove bad columns', and 'Position...'. The main workspace contains a workflow diagram with a 'Reader 0' block connected to four 'Phy image' blocks labeled 'Chip0_0_0', 'Chip1_0_0', 'Chip2_0_0', and 'Chip3_0_0'. A progress dialog box is open, displaying a 15% progress indicator and the text 'Reading dump from reader...'. The dialog also lists 'Chip: Chip0', 'Port: 0', and 'Crystal: 0', with a 'Cancel' button at the bottom.

Visual NAND R

Case Workspace Plugins

Delete Copy Open images Insert area Skip area Extract area Remove bad columns Positi...

Element functions

Workspace X

Reader 0

Phy image Chip0_0_0

Phy image Chip1_0_0

Phy image Chip2_0_0

Phy image Chip3_0_0

15% Reading dump from reader...

Chip: Chip0
Port: 0
Crystal: 0

Cancel

DHCP leases log

Name	Size	Files	Last Modified	Allocated	Type	Folders
3 MB G:\UBIFS\CALIX\ on [NV_SSD]	3 MB	53	19/05/2022 17:36:35	3 MB	Folder	25
3 MB Files-volume-1	3 MB	27	19/05/2022 17:36:35	3 MB	Folder	19
3 KB udhcpd	3 KB	2	19/05/2022 17:36:35	4 KB	Folder	0
459 Bytes udhcpd.conf	459 Bytes	1	05/08/2021 01:31:34	0 Bytes	CONF File	0
2 KB udhcpd.leases	2 KB	1	05/08/2021 01:31:34	4 KB	LEASES File	0
2 KB poe	2 KB	1	19/05/2022 17:36:35	4 KB	File	0
3 MB log	3 MB	5	19/05/2022 17:36:35	3 MB	Folder	0
512 KB messages.0	512 KB	1	23/07/2021 23:17:16	516 KB	0 File	0
512 KB messages.1	512 KB	1	12/07/2021 09:47:50	516 KB	1 File	0
512 KB messages.2	512 KB	1	12/07/2021 01:45:48	516 KB	2 File	0
512 KB messages.3	512 KB	1	11/07/2021 17:28:54	516 KB	3 File	0
512 KB messages.4	512 KB	1	07/07/2021 06:39:30	516 KB	4 File	0
33 KB delta_1	33 KB	5	19/05/2022 17:36:35	36 KB	Folder	3
33 KB delta_0	33 KB	5	19/05/2022 17:36:35	36 KB	Folder	3
0 Bytes arc	0 Bytes	0	19/05/2022 17:36:35	0 Bytes	Folder	6
68 KB [9 Files]	68 KB	9	05/08/2021 01:31:33	80 KB		0
1 KB log_message	1 KB	1	05/08/2021 01:31:33	4 KB	File	0
3 KB smact_data.json	3 KB	1	05/08/2021 01:31:33	4 KB	JSON File	0
8 KB scratchpad	8 KB	1	05/08/2021 01:31:31	8 KB	File	0
32 Bytes running_uptime	32 Bytes	1	05/08/2021 01:31:09	0 Bytes	File	0
183 Bytes upgrade_log.dat	183 Bytes	1	05/05/2021 08:04:39	0 Bytes	DAT File	0
826 Bytes var_log_128k_mapagent_saved	826 Bytes	1	05/05/2021 08:03:21	4 KB	File	0
3 KB wlanmgr_log_messages_saved	3 KB	1	05/05/2021 08:03:21	4 KB	File	0
46 KB var_log_messages_reset_saved	46 KB	1	05/05/2021 08:03:20	48 KB	File	0

DHCP leases log

udhcpd.leases

MAC Addresses

Leased IP Addresses

Device name

0000	C8 52 61	00 00 00 00 00 00 00 00	C0 A8 FA 0A	00 00 00 00 00 00 00 00		
0058	18 9C 27	00 00 00 00 00 00 00 00	C0 A8 FA 0B	00 00 00 00 00 00 00 0051 71 44 56 52 5F 57 49 46 49 5F 31 38 3A 39 63 3A 32 37 3A 39 62QqDVR_WIFI_18:9c:27	
00B0	00 E0 4C	00 00 00 00 00 00 00 00	C0 A8 FA 0C	00 00 00 00 00 00 00 00
0108	58 E6 BA	00 00 00 00 00 00 00 00	C0 A8 FA 0D	00 00 00 00 69 50 68 6F 6E 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00iPhone.....
0160	BC 77 37	00 00 00 00 00 00 00 00	C0 A8 FA 0E	00 00 00 00 4F 6C 69 76 65 72 00 00 00 00 00 00 00 00 00 00 00 00 00 00Oliver.....
0188	18 9C 27	00 00 00 00 00 00 00 00	C0 A8 FA 0F	00 00 00 00 4E 4F 44 45 5F 57 49 46 49 5F 31 38 3A 39 63 3A 32 37NODE_WIFI_18:9c:27
0210	18 9C 27	00 00 00 00 00 00 00 00	C0 A8 FA 10	00 00 00 00 4E 4F 44 45 5F 57 49 46 49 5F 31 38 3A 39 63 3A 32 37NODE_WIFI_18:9c:27
0268	18 9C 27	00 00 00 00 00 00 00 00	C0 A8 FA 11	00 00 00 00 4E 4F 44 45 5F 57 49 46 49 5F 31 38 3A 39 63 3A 32 37NODE_WIFI_18:9c:27
02C0	18 9C 27	00 00 00 00 00 00 00 00	C0 A8 FA 12	00 00 00 00 4E 4F 44 45 5F 57 49 46 49 5F 31 38 3A 39 63 3A 32 37NODE_WIFI_18:9c:27
0318	A4 11 62	00 00 00 00 00 00 00 00	C0 A8 FA 13	00 00 00 00 56 4D 42 34 35 30 30 00 00 00 00 00 00 00 00 00 00 00 00 00VMB4500.....
0370	14 FE B5	00 00 00 00 00 00 00 00	C0 A8 FA 14	00 00 00 00 4F 6C 69 76 65 72 00 00 00 00 00 00 00 00 00 00 00 00 00 00Oliver.....
03C8	1C BF C0	00 00 00 00 00 00 00 00	C0 A8 FA 15	00 00 00 00 4C 41 50 54 4F 50 2D 45 56 49 43 43 37 48 43 00 00 00 00 00 00LAPTOP-EVICC7HC.....
0420	86 CA A3	00 00 00 00 00 00 00 00	C0 A8 FA 16	00 00 00 00 47 61 6C 61 78 79 2D 53 39 00 00 00 00 00 00 00 00 00 00 00Galaxy-S9.....
0478	48 D2 24	00 00 00 00 00 00 00 00	C0 A8 FA 17	00 00 00 00 44 45 53 48 54 4F 50 2D 42 45 41 37 4C 42 4E 00 00 00 00 00 00DESKTOP-BEA7LBN.....
0400	7C 05 07	00 00 00 00 00 00 00 00	C0 A8 FA 18	00 00 00 00 44 45 53 48 54 4F 50 2D 42 45 41 37 4C 42 4E 00 00 00 00 00 00DESKTOP-BEA7LBN.....
0528	80 86 D9	00 00 00 00 00 00 00 00	C0 A8 FA 19	00 00 00 00 47 61 6C 61 78 79 2D 54 61 62 2D 41 00 00 00 00 00 00 00 00Galaxy-Tab-A.....
0580	A0 C9 A0	00 00 00 00 00 00 00 00	C0 A8 FA 1A	00 00 00 00 47 61 6C 61 78 79 2D 53 38 00 00 00 00 00 00 00 00 00 00 00Galaxy-S8.....
05D8	6E 7F 08	00 00 00 00 00 00 00 00	C0 A8 FA 1B	00 00 00 00 69 50 68 6F 6E 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00iPhone.....
0630	0C 89 10	00 00 00 00 00 00 00 00	C0 A8 FA 1C	00 00
0688	A4 C3 F0	00 00 00 00 00 00 00 00	C0 A8 FA 1D	00 00
06E0	F8 0F F9	00 00 00 00 00 00 00 00	C0 A8 FA 1E	00 00 00 00 43 68 72 6F 6D 65 63 61 73 74 2D 55 6C 74 72 61 00 00 00 00 00Chromecast-Ultra.....
0738	F8 0F F9	00 00 00 00 00 00 00 00	C0 A8 FA 1F	00 00 00 00 47 6F 6F 67 6C 65 2D 4E 65 73 74 2D 4D 69 6E 69 00 00 00 00 00Google-Nest-Mini.....
0790	68 57 2D	00 00 00 00 00 00 00 00	C0 A8 FA 20	00 00 00 00 77 6C 61 6E 30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00wlan0.....
07E8	48 3F DA	00 00 00 00 00 00 00 00	C0 A8 FA 21	00 00 00 00 45 53 50 5F 38 46 37 36 44 45 00 00 00 00 00 00 00 00 00 00ESP_8F76DE.....
0840	18 69 D8	00 00 00 00 00 00 00 00	C0 A8 FA 22	00 00 00 00 77 6C 61 6E 30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00wlan0.....
0898	56 1F 24	00 00 00 00 00 00 00 00	C0 A8 FA 23	00 00 00 00 50 61 75 6C 73 2D 47 61 6C 61 78 79 2D 53 39 00 00 00 00 00 00Pauls-Galaxy-S9.....
08F0	3C 7C 3F	00 00 00 00 00 00 00 00	C0 A8 FA 24	00 00 00 00 44 45 53 48 54 4F 50 2D 55 52 38 41 54 42 41 00 00 00 00 00 00DESKTOP-UR8ATBA.....
0948	04 6C 59	00 00 00 00 00 00 00 00	C0 A8 FA 25	00 00 00 00 44 45 53 48 54 4F 50 2D 55 52 38 41 54 42 41 00 00 00 00 00 00DESKTOP-UR8ATBA.....
09A0	00 26 86	00 00 00 00 00 00 00 00		

One record

Lease time, sec

```
udhcpd.conf - Notepad
File Edit Format View Help
decline_file /var/udhcpd.decline
auto_time 900
interface br0
start 192.168.250.10
end 192.168.250.200
option lease 86400
min_lease 30
option subnet 255.255.255.0
option router 192.168.250.1
option dns 192.168.250.1
option dns 192.168.250.1
option domain Home
interface brqt
start 169.254.1.2
end 169.254.1.2
option lease 86400
min_lease 30
option subnet 255.255.255.0
option router 169.254.1.1
option dns 169.254.1.1
option dns 169.254.1.1
option domain Home
```


Thank you!!!