

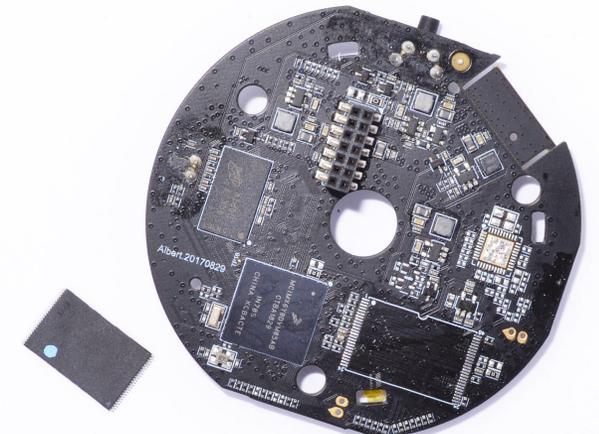
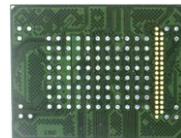
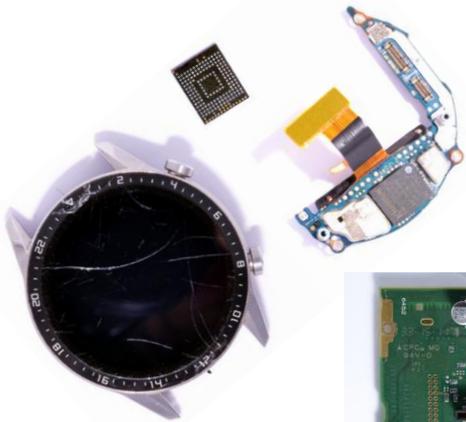
Advanced Forensics IoT & Vehicle Forensics

Alexander Sheremetov

Rusolut, Poland

A New Digital Forensics Era

It's not just mobile forensics anymore. There are much more data sources than we used to know. Embedded systems do not always have the interface connectors. Working with the memory chip directly gives a full access to memory and data.



Vehicle forensics – Infotainment systems



Every modern car has at least one data source, sometimes two or more. The phone normally connects through Bluetooth and lots of data gets synchronized: phone ID data, contact book, call logs, sms, etc. If the system supports GPS, then such data as last destination, trips, fuel data, etc are stored in the computer. Car event logs also help to establish the facts of activity.

Mercedes AMG C43 - Multimedia Interface Control Unit



 **Mercedes-Benz** A 222 900 48 19 / 001
Hardware for Enhanced Remote-, Mobility- & Emergency Services

Model:	HERMES 1.5	ID:	0700 A 222 901 82 06 ZGS(HW): 001 17/37
Version:	LTE NAFTA	EC:	100 A 222 902 72 18 ZGS(SW): 001 18/03
Type No:	M197	Serial No.:	J263 Q01
WLAN - MAC:	2C9CADF	Date of Manufacture:	2018/10/10
NAD SW:	11.787.01.00.1419		
IMEI:	35418908		
ICCID:	8901170427250		
12V	0.5A		

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: Q1SME919BS - 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 UNDESIRE OPERATION.

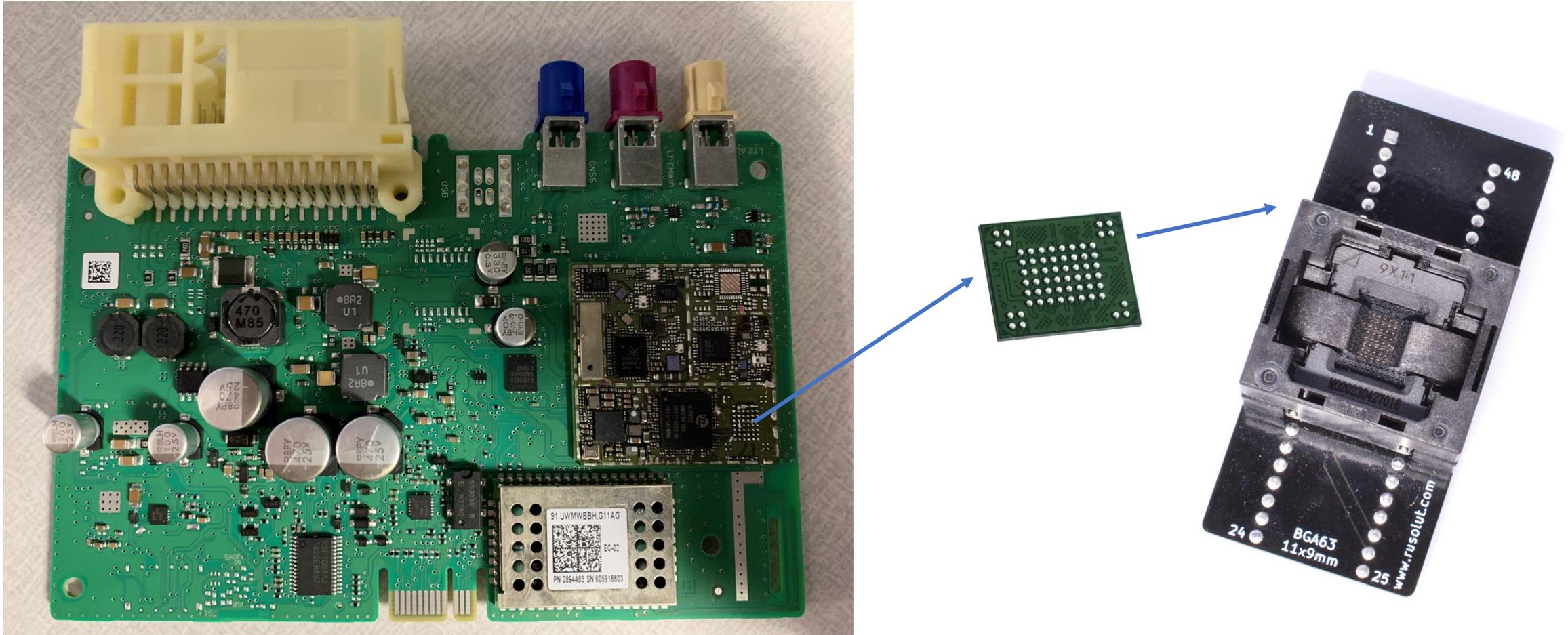
Harman Becker Automotive Systems GmbH
Becker - Göring - Straße 16
76307 Karlsbad, Germany
Manufactured in Hungary


M197J80J263

<https://cdn.carbuzz.com/gallery-images/2019-mercedes-amg-c43-sedan-dashboard-carbuzz-508885.jpg>

Inside Multimedia Interface Control Unit – PCB and memory



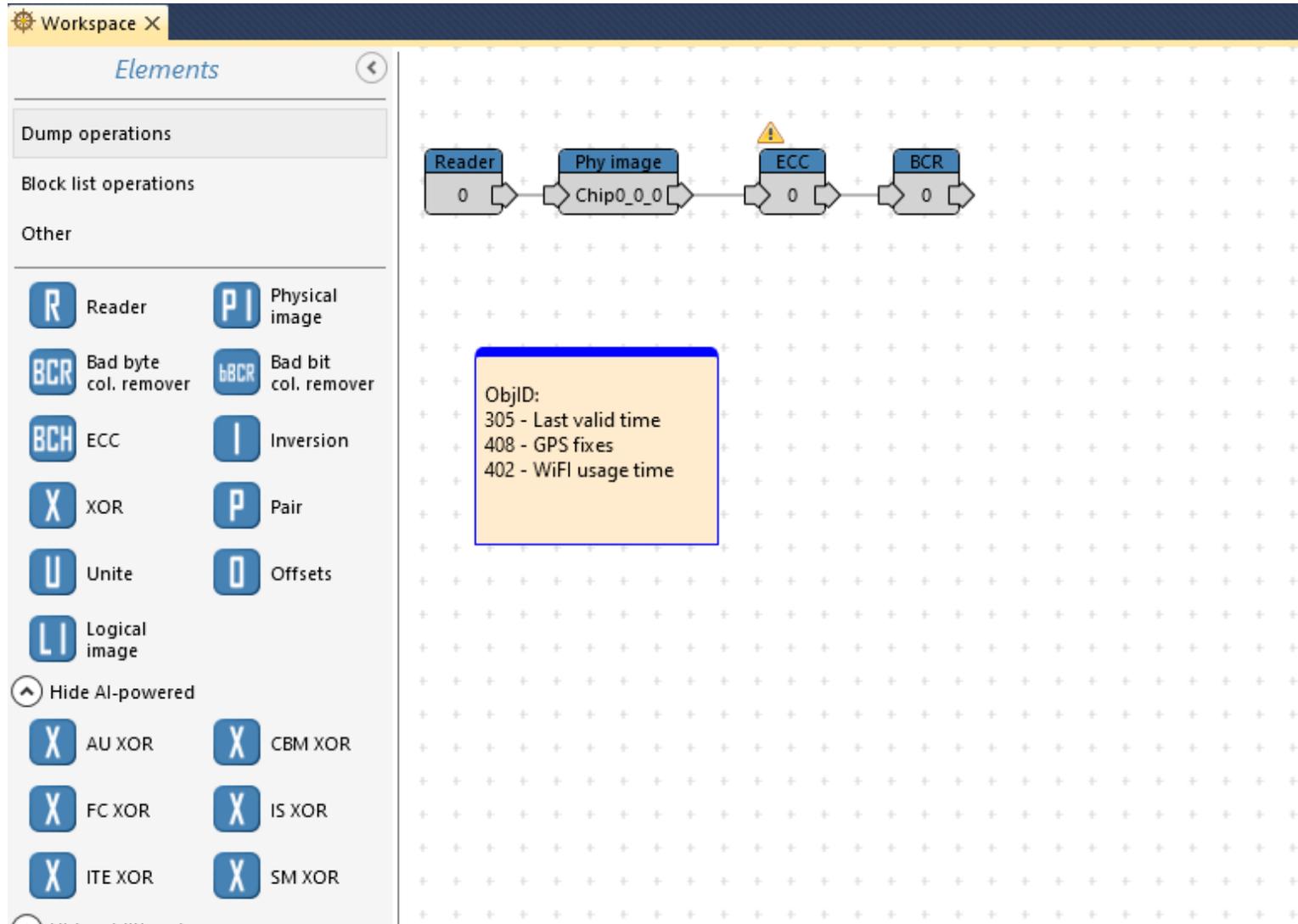
The unit was disassembled and the BGA63 NAND memory chip was extracted using chip-off technique. The memory chip then was plugged into special BGA63 adapter of Visual NAND Reconstructor.

NAND memory in the VNR Reader



Most of flash memory chips can be read in VNR reader through easy-to-use adapter

NAND memory dump reading and processing



YAFFS2 file system parser – besides user's data, the car's events are also stored for a long time

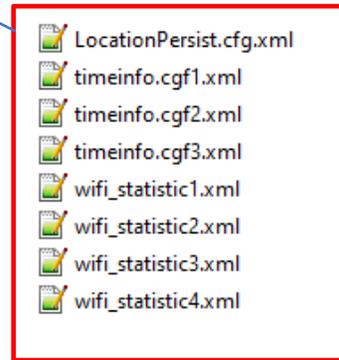
The screenshot displays the YAFFS2 file system parser interface. At the top, there are control panels for 'Meta data offset' (0), 'Sequence number offset' (2048), 'Object Id offset' (2052), 'Chunk Id offset' (2056), 'Byte count offset' (2060), 'Block status offset', and 'Data status offset'. There are also buttons for 'Read SA', 'Byte order', and 'Sync with dump'. Below this is a table listing file system entries with columns for Use, Chur, Object Type, Object Id, Chunk Id, Sequence number, Byte count, Parent, Name, Permission, UID, GID, atime, mtime, ctime, File size, and Address. The table shows various file headers and data blocks, including 'onoff.log' and multiple 'wifi_statistic.xml' files.

Use	Chur	Object Type	Object Id	Chunk Id	Sequence number	Byte count	Parent	Name	Permission	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	0x5D798B94	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	0x5D798B9B	0x15D	0x001FE690C0
✓	0x80	File header (0x10)	0x000402	0x000401	0x000041D4	0x015D	0x401	wifi_statistic.xml	0x81B0	0x3E8	0x3E8	0x135	0x5D798B9B	0x5D798B9B	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

Below the table is a hex dump of data. The dump shows hexadecimal values in columns 00-0F and corresponding ASCII characters. A red box highlights a specific line in the dump: 2019-03-07 02:13:31 [13.064] GAU:cycle<9>;setDTC watchdogReset WUR<0x2000> last entry: <>.2020-02-23 01:56:08 [13.189] GAU:cycle<39>;setDTC watchdogReset WUR<0x2000> last entry: <>.2020-02-23 01:56:08 [13.189] GAU:cycle<39>;setDTC watchdogReset WUR<0x2000> last entry: <>.....

Data extracted from the file system

```
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
}
```

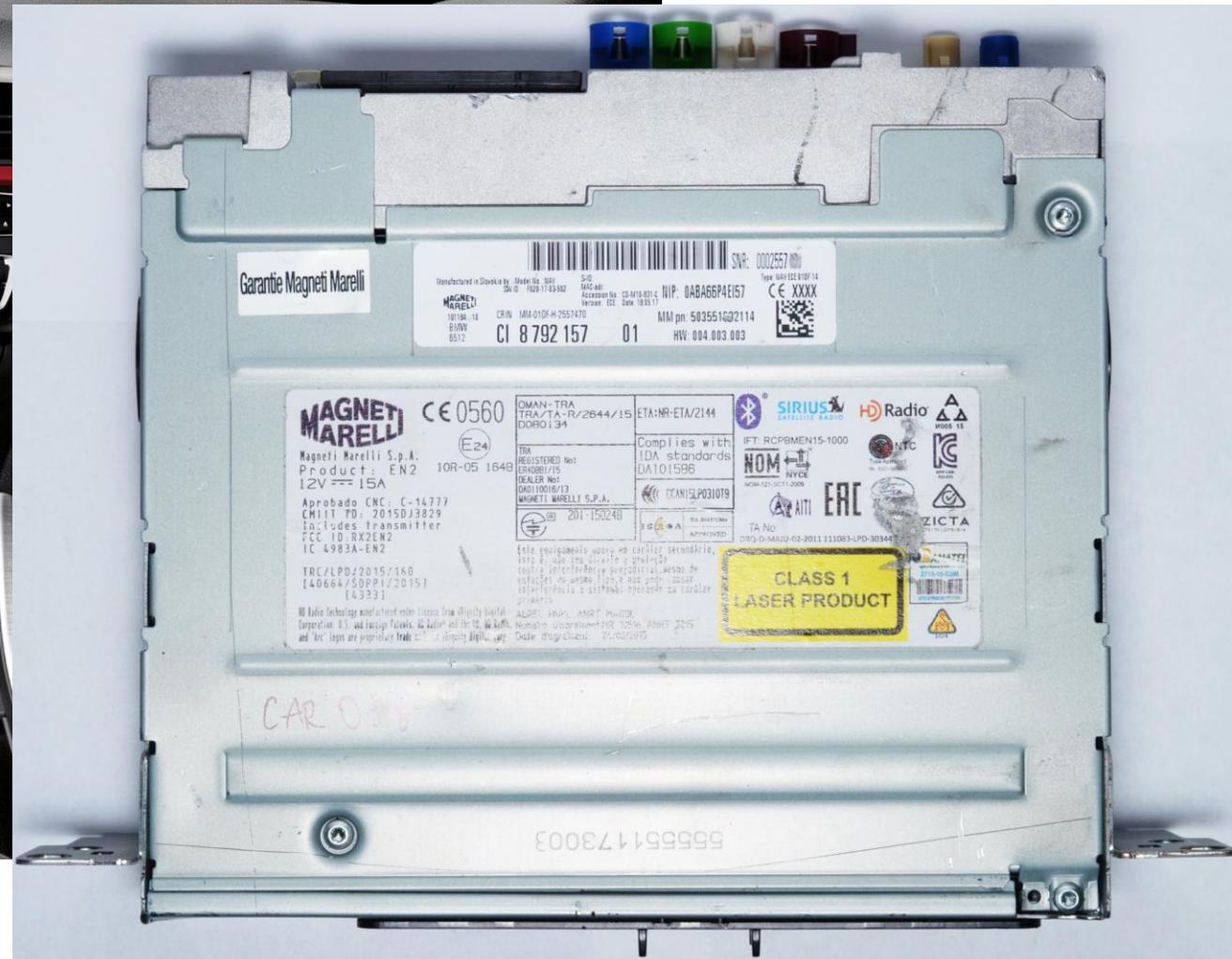


```
timeinfo.cgf1.xml
TimeInfo
{
  version 1
  deltaValue 4294945688
  lastValidTime 1567867559
}
```

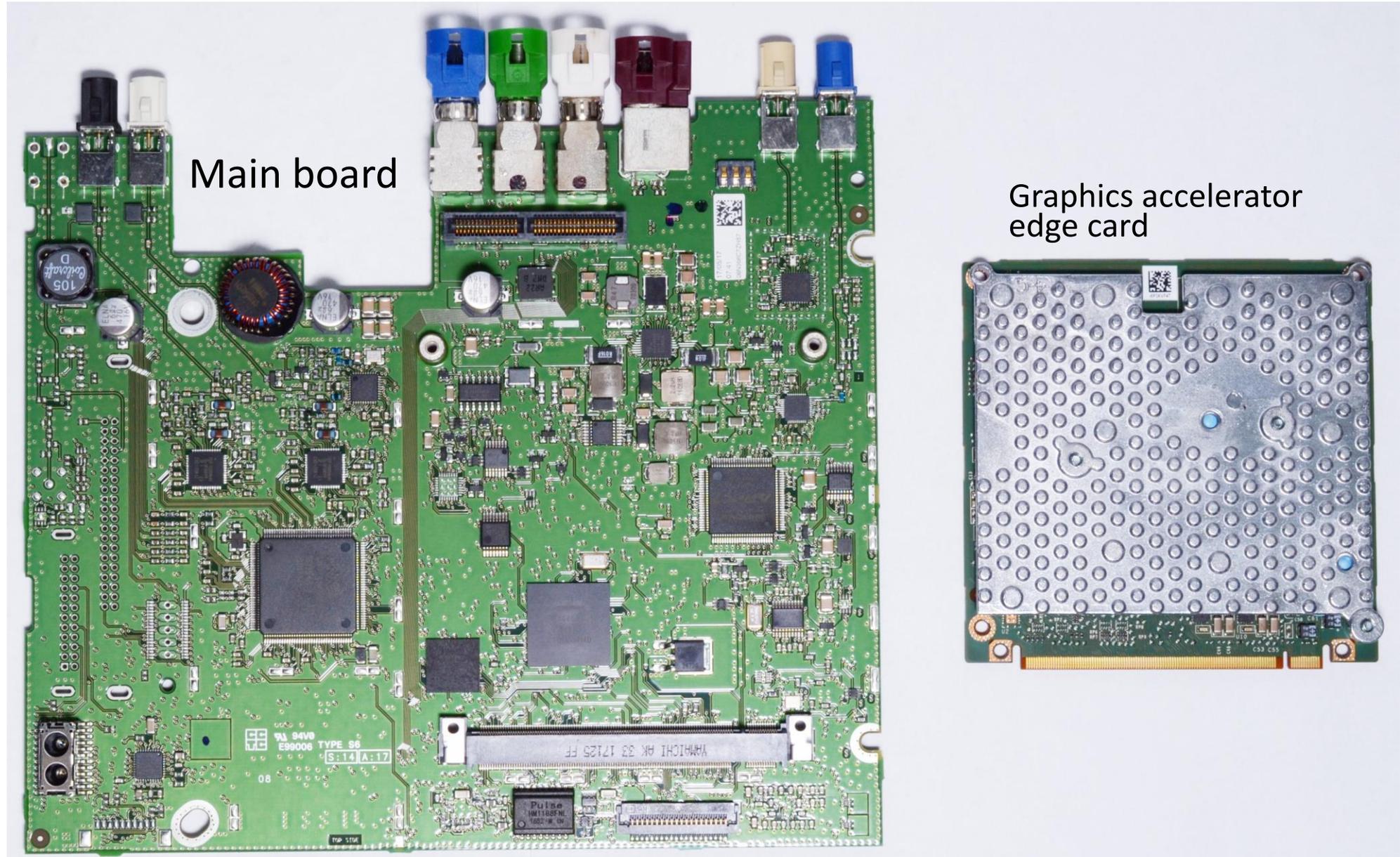
```
wifi_statistic1.xml
<?xml version="1.0" encoding="UTF-8"?>
<config>
  <total_connected_time>904902</total_connected_time>
  <total_rx>191936195</total_rx>
  <total_tx>124303838</total_tx>
  <total_flow>316240033</total_flow>
  <curr_connected_time>3006</curr_connected_time>
  <curr_rx>738407</curr_rx>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

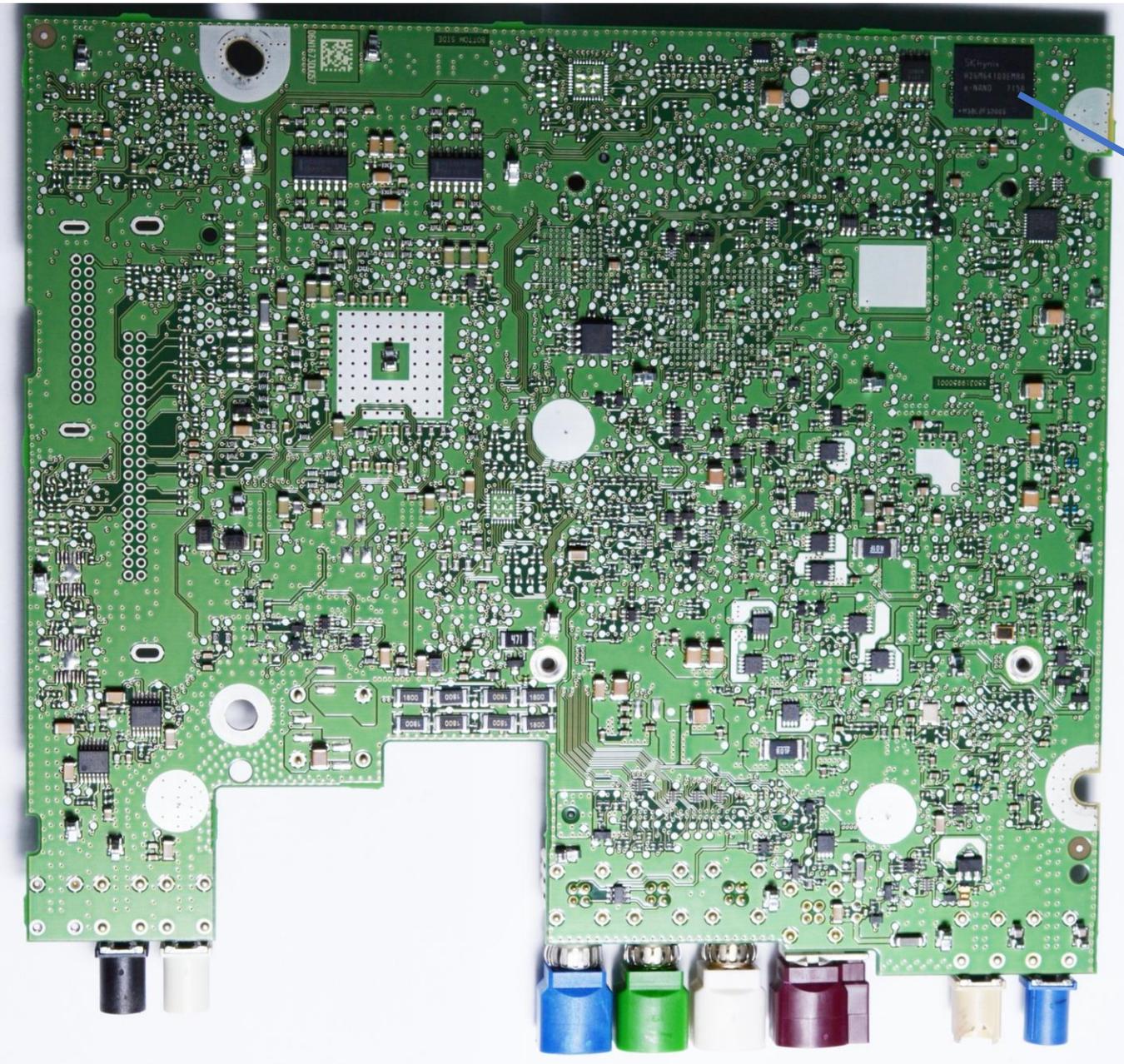
The memory chip holds a vast amount of the navigation data, such as **Last destinations** with **timestamps**

BMW 3 F30 Infotainment system



Internal boards extracted from the Infotainment system

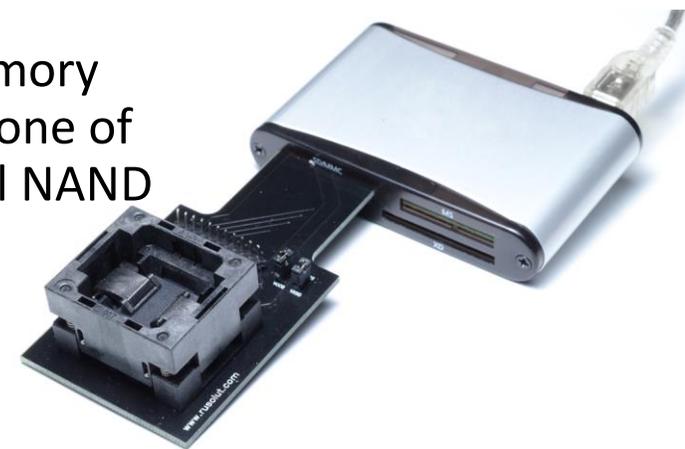




The eMMC memory chip BGA169/153 on the Main board



Classic eMMC memory can be read using one of adapters for Visual NAND Reconstructor



The memory is recognized in eMMC adapter and can be imaged

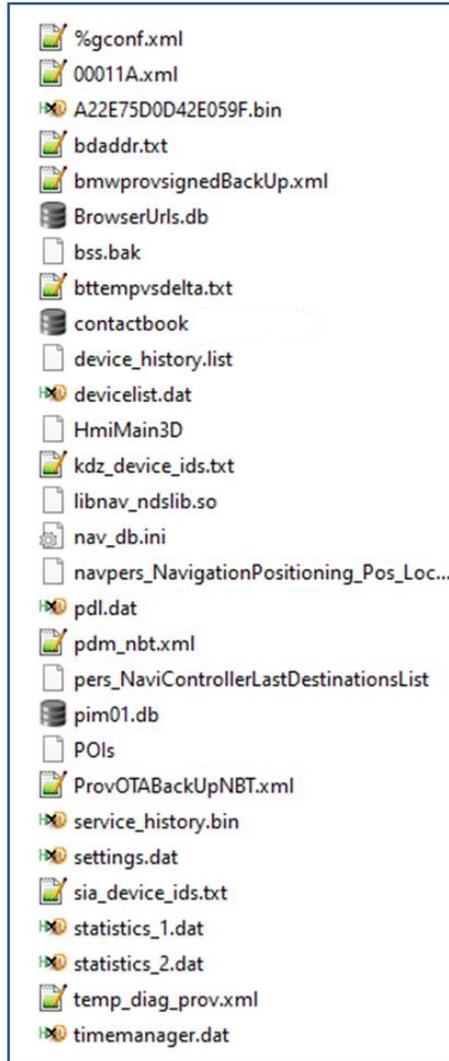
The screenshot displays the Visual Nand Reconstructor (VNR) software interface. The window title is "Visual Nand Reconstructor - Case". The interface is divided into several sections:

- 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 showing a diagram of the volume partitioning scheme. The diagram consists of a sequence of boxes: "Reader" (0), "Phy image" (TSOP48), "ECC" (0), "Offsets" (0), and "Data area" (0). Below this, there is a diagram showing "eMMC" (0) connected to "Copy" (0), with red warning icons above each.
- Dump:** A tree view on the left showing the file system structure. It includes "MBR" and several "Volume" entries (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".

The workspace diagram illustrates the volume partitioning scheme, showing a sequence of components: Reader (0), Phy image (TSOP48), ECC (0), Offsets (0), and Data area (0). Below this, a diagram shows eMMC (0) connected to Copy (0), with red warning icons above each, indicating a potential issue or warning.

The volume partitioning scheme consists of multiple EXT volumes and can be parsed in VNR with full structure

Plenty of files extracted from file system of eMMC



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	76Devicelist 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	YYYY....cëCC: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	00	: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	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	YYYY.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	3A00:0
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	FF	YYYYYYYYYYYYYYY
00000256	FF	FF	FF	FF	00	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	YYYY.YYYYYYYYYYYY
00000272	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	00	00	00	YYYYYYYYYYYYYYY....
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	3A00:00:00:00:
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	FF	YYYYYYYYYYYYYYY.YYY
00000368	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	YYYYYYYYYYYYYYYYYYY
00000384	FF	FF	FF	FF	00	00	00	00	00	00	00	00	00	00	00	00	YYYY.....
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	00	30	30	3A00:0
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	FF	YYYYYYYYYYYYYYYYYYY
00000464	FF	FF	FF	FF	00	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	YYYY.YYYYYYYYYYYY
00000480	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	00	00	00	YYYYYYYYYYYYYYY....
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

Device list of connected phones with their BT mac addresses

Call log history of connected phones with timestamps

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...6áyyyZ....
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	33	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	33	..01.07.19.....+4850345 355	

Offset: 0

Overwrite

Last destinations log

FP sList

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	00	03	0E	c.>.y..î.....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~Û#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~Û#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.....³.....:pû#œ>
00001024	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.....;*¿#œÿ.....C:	
00001056	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	
00001088	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	Å.KU LOTNICZEGO H:13 R:31-868...	
00001120	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.....	
00001152	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.....;*¿#œÿ.....	
00001184	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.	
00001216	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..	
00001248	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.....	
00001280	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	
00001312	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.. .1.#~?ý.y.y.î.....£.	
00001344	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	981.#~?ý.....0Eÿ#~	
00001376	35	EC	00	00	00	00	0E	31	5F	DF	23	98	47	8A	00	00	00	00	0E	31	21	16	23	98	3C	A2	00	00	00	00	02	43	5i.....l_B#~GŠ.....l!.#~<c.....C	
00001408	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	
00001440	4B	41	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	00	KA.....1.#~?ý.....	
00001472	05	00	00	00	02	0E	30	8C	DD	23	98	35	EC	00	00	00	00	0E	31	5F	DF	23	98	47	8A	00	00	00	00	02	00	050Eÿ#~5i.....l_B#~GŠ.....	
00001504	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..	
00001536	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.WIĄŚNIA"WKA MASÅ.Å"	
00001568	57	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	00	W.....607695030.246668986....	
00001600	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.....WIĄŚNIA"WKA....	
00001632	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..	
00001664	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	
00001696	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:WIĄŚNIA"WKA R:MASÅ.Å"W..	
00001728	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	00P°\$8°q.....	

Offset: 0

Overwrite

Phonebook – phone numbers and attributes

Case SQLite carver

Export Remove duplicates Remove unselected

SQLite carver phone_data_phone X Master Table Phy image contactbook_20120928 Workspace

Source
Dump
Template
Search
Start address 0

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"/>	2	2	0	0	3	575241	75241	5 237545	N1 N2 N3 N4 N5 S6 N7	
<input checked="" type="checkbox"/>	3	3	0	0	3	+48501568	1568	7 237518	N1 N2 N3 N4 N5 S6 N7	
<input checked="" type="checkbox"/>	4	4	0	0	3	+48501968	1968	4 237491	N1 N2 N3 N4 N5 S6 N7	
<input checked="" type="checkbox"/>	5	5	0	0	3	+48602713	2713	9 237464	N1 N2 N3 N4 N5 S6 N7	
<input checked="" type="checkbox"/>	6	6	0	0	3	+48601586	1586	8 237437	N1 N2 N3 N4 N5 S6 N7	
<input checked="" type="checkbox"/>	7	7	0	0	3	1111	11	237419	N1 N2 N3 N4 N5 S6 N7	
<input checked="" type="checkbox"/>	8	8	0	0	3	+487988	988	083 237391	N1 N2 N3 N4 N5 S6 N7	
<input checked="" type="checkbox"/>	9	9	0	0	3	692051	92051	9 237366	N1 N2 N3 N4 N5 S6 N7	
<input checked="" type="checkbox"/>	10	10	0	0	3	+48531	31168	9 237338	N1 N2 N3 N4 N5 S6 N7	
<input checked="" type="checkbox"/>	11	11	0	0	3	+48517918	17918	9 237310	N1 N2 N3 N4 N5 S6 N7	
<input checked="" type="checkbox"/>	12	12	0	0	3	+4850675	675	0 237283	N1 N2 N3 N4 N5 S6 N7	
<input checked="" type="checkbox"/>	13	13	0	0	3	509089	9089	7 237258	N1 N2 N3 N4 N5 S6 N7	
<input checked="" type="checkbox"/>	14	14	0	0	3	601777	1777	9 237234	N1 N2 N3 N4 N5 S6 N7	
<input checked="" type="checkbox"/>	15	15	0	0	3	+487940	94041	2 237206	N1 N2 N3 N4 N5 S6 N7	
<input checked="" type="checkbox"/>	16	16	0	0	3	+4888555	8555	7 237178	N1 N2 N3 N4 N5 S6 N7	
<input checked="" type="checkbox"/>	17	17	0	0	3	+4850290	2906	4 237151	N1 N2 N3 N4 N5 S6 N7	
<input checked="" type="checkbox"/>	18	18	0	0	3	+4884627	4627	30 237123	N1 N2 N3 N4 N5 S6 N7	
<input checked="" type="checkbox"/>	19	19	0	0	3	5035211	35211	44 237099	N1 N2 N3 N4 N5 S6 N7	
<input checked="" type="checkbox"/>	20	20	0	0	3	660047	60047	51 237074	N1 N2 N3 N4 N5 S6 N7	
<input checked="" type="checkbox"/>	21	21	0	0	3	+48515	1530	69 237046	N1 N2 N3 N4 N5 S6 N7	
<input checked="" type="checkbox"/>	22	22	0	0	3	+486964	9645	45 237018	N1 N2 N3 N4 N5 S6 N7	
<input checked="" type="checkbox"/>	23	23	0	0	3	783959	8395	08 236993	N1 N2 N3 N4 N5 S6 N7	

Position 1 from 660

The **phonebook of Bluetooth connected phone** is recovered with full structure of SQLite tables. The memory chip may have vast array of data even from very old events of connected devices, since erase operation on the memory is almost a taboo, due to limited lifespan of the NAND.

Phonebook - Names

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

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

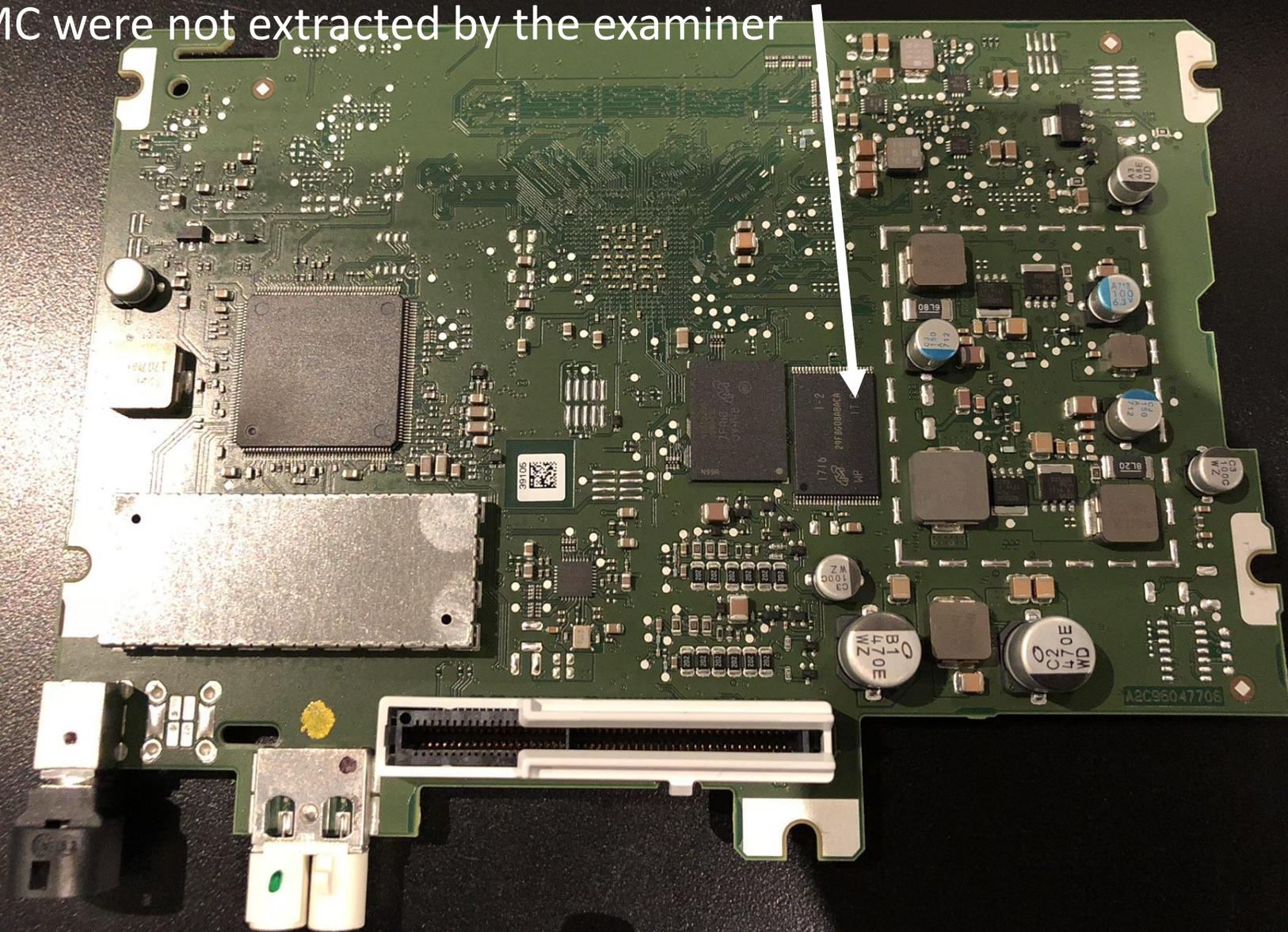
The **names** are stored in separate table but can be easily combined with numbers.

This kind of evidence is priceless when attempting to establish the forensic facts.

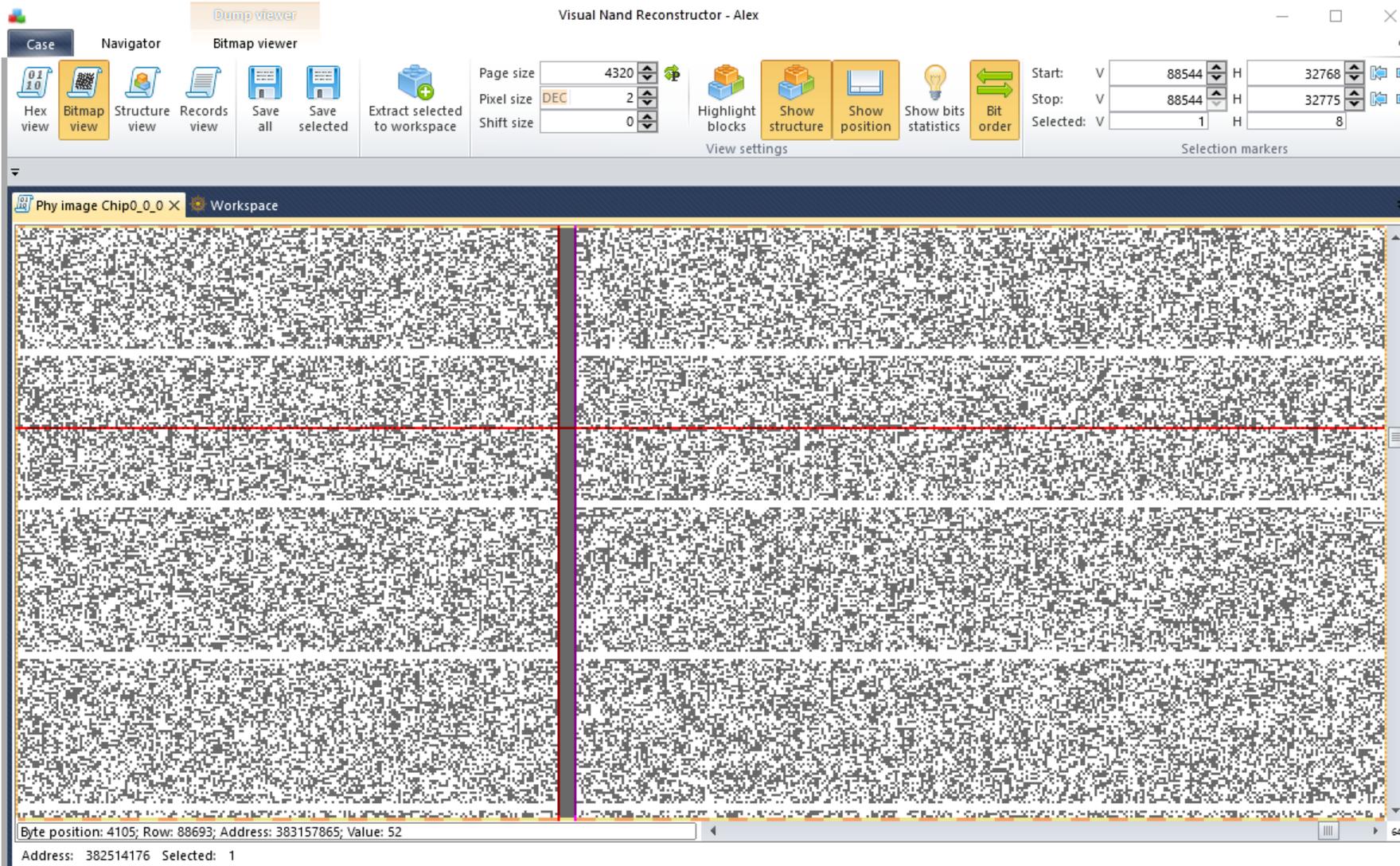
Citroen C3 Aircross



We got the physical images from the chips extracted by our user.
It was Continental NAC_EUR_WAVE2 computer.
Single 1GB Micron 29F8G08ABACA TSOP48 chip. Dumps from the
eMMC were not extracted by the examiner

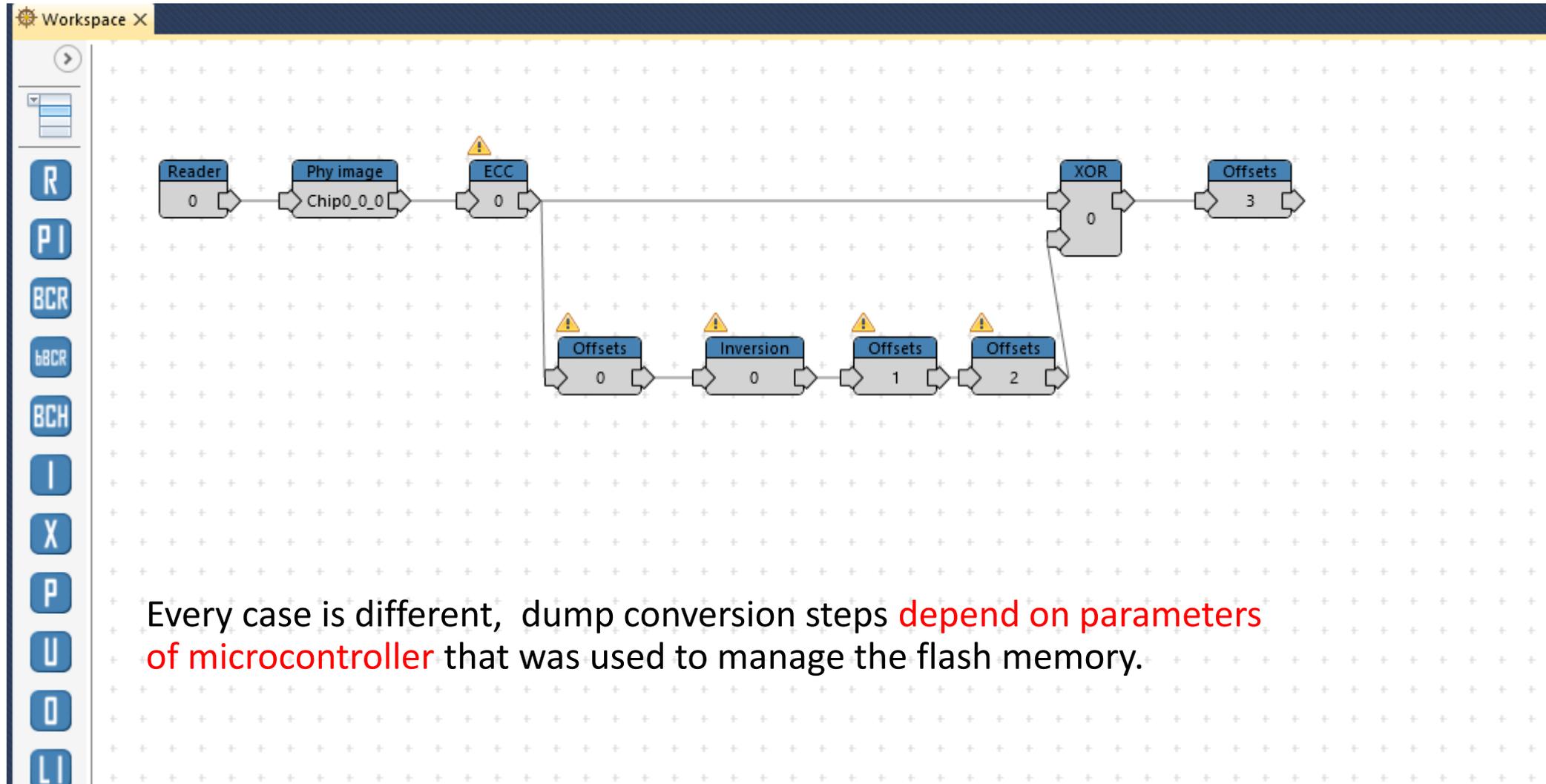


The memory dump through the bitmap



The bitmap helps to analyze and separate spare area of memory from the actual user's data area.

Emulation of controller's conversion workflow



UBIFS file system was used to manage the data in flash memory

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	00iiöb.....
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	F7ÿ*
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	ÿÿ\,i=iR~f.*ÿ°ÿ
000F5BE210	F2	54	A8	A8	A8	6F	0B	92	24	1F	00	00	00	00	00	00	øT""o.'ÿ.....
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:

The most important data in this case was related to GPS navigation and routes of the car owner.

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

Mode: Binary

```
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 .... @K . i . ; y . . (
00b0 4d fc e3 15 01 ff ff ff ff ff ff ff ff 01 N
```

Dozens of records with **last historical destinations** were pulled out of the device.



2 My Ladys Rd

- Wyznacz trasę
- Zapisz
- W pobliżu
- Wyślij na telefon
- Udostępnij

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 miejsca
- Dodaj swoją firmę
- Dodaj etykietę

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

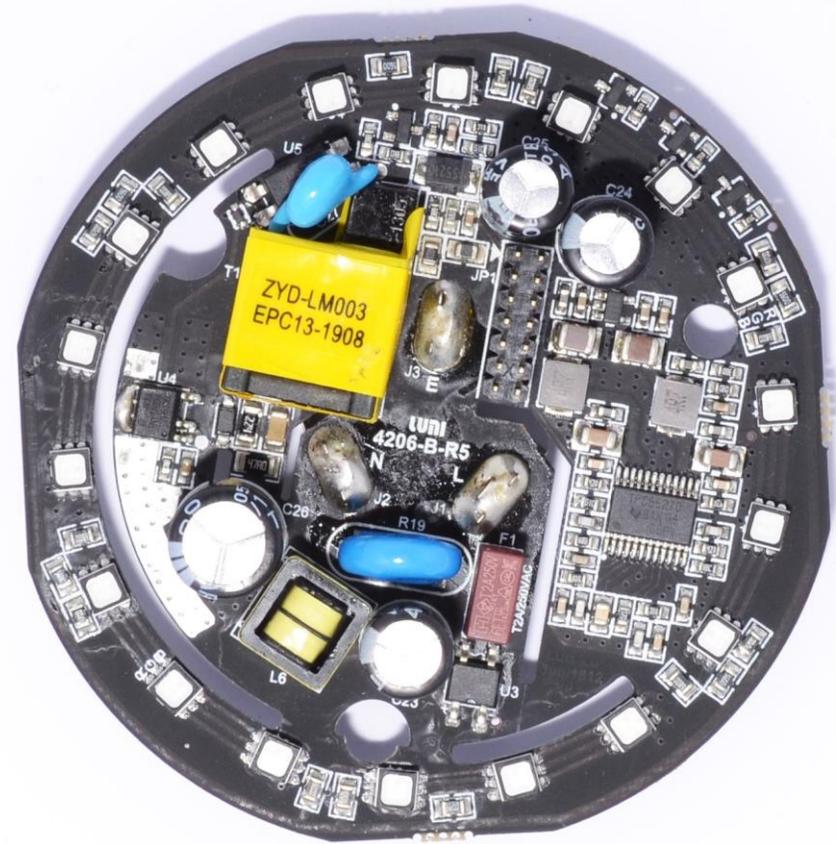
Apply

Xiaomi smart home gateway/hub V2 DGNWG05LM



The device is used as a Wi-Fi, ZigBee and Bluetooth hub for the smart home sensors and automations (e.g. motion sensor, door lock sensor, water sensor, cameras, etc)

Analog PCB both sides

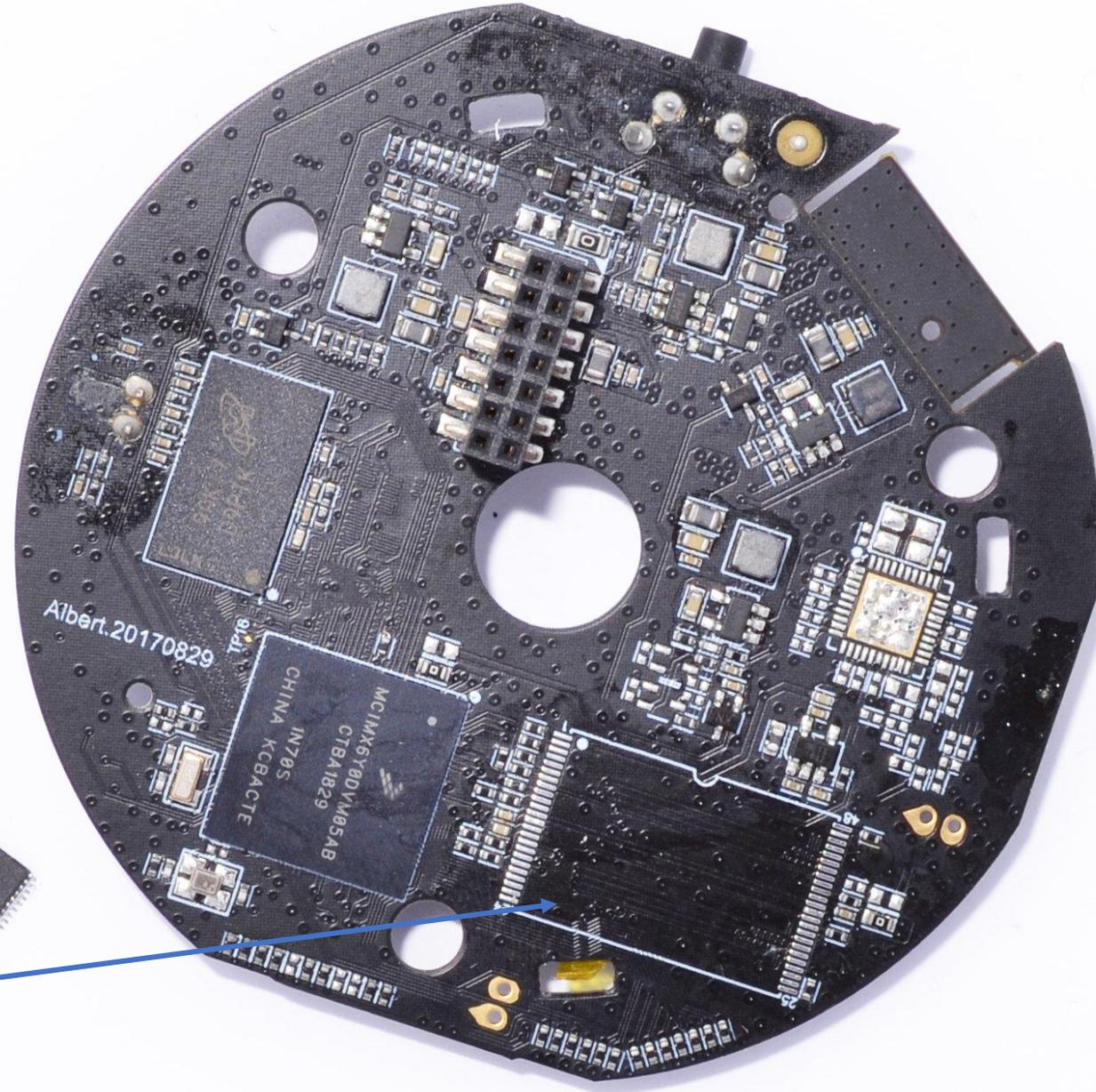


The hub consists of two PCBs connected together. Analog PCB has nothing interesting since it's only power-related. Its functions are to convert AC from the wall socket to the digital board, power management, pwm led controller, leds, etc)

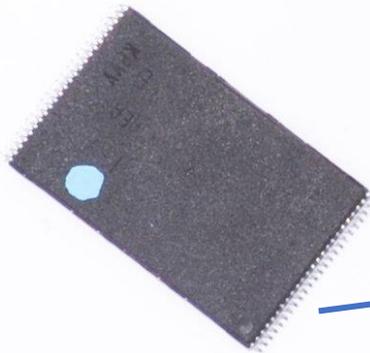
Digital PCB top side (ZigBee, Wi-Fi modules)



Digital PCB bottom side (MCU, NAND, RAM)



TSOP48 NAND



The NAND memory was read via VNR reader

The screenshot displays the Visual Nand Reconstructor (VNR) software interface. The title bar reads "Visual Nand Reconstructor - XiaomiV2_DGNWG05LM_SashaHome". The interface includes a menu bar with "Case", "Workspace", "Plugins", and "Databases". Below the menu is a toolbar with icons for "Delete", "Copy", "Paste", "Open images", "Send solution to Db", "Insert area", "Skip area", "Extract area", and "Position...". The "Solution" panel on the right shows the following details:

- Solution type: Controller:
- Device type: Memory chip ID: 2CDA909506
- Device name: Number of memory chips: 1
- Pinout: Number of crystals: 1

The main workspace shows a workflow diagram on a grid background. The workflow consists of the following steps:

- Reader** (ID: 0)
- Phy image** (ID: Chip0_0_0)
- ECC** (ID: 0)
- Offsets** (ID: 1 byte)
- Offsets** (ID: 2038 bytes)
- Offsets** (ID: 35 bytes)
- Concatenate** (ID: 0)
- Offsets** (ID: 0)
- Copy** (ID: 0)

Each step is represented by a blue box with a yellow warning triangle icon. The workflow is connected by arrows, indicating the flow of data from the Reader to the final Copy step.

On the left side of the workspace, there is a vertical toolbar with icons for various reconstruction algorithms: R, PI, BCR, bBCR, BCH, I, X, and P.

At the bottom of the interface, there is an "Event log explorer" panel and a status bar showing "Last active selection: address" and "selected". The version number "0.20" is also visible in the bottom right corner.

Controller's data-to-memory channel reconstruction for further data extraction

UBIFS file system volume (device was possibly reset, since many lost iNodes)

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

Copy 0 X Workspace

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

Address: 270597918 Selected: 0

	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".."e./e".."
00102101C0	90	13	2F	90	93	22	05	10	03	43	2D	80	26	01	CB	01	□./□"..."C-ε&.È.
00102101D0	2E	C1	17	41	2A	40	1F	01	17	41	2A	80	1E	41	16	41	.Ä.A*@...A*ε.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	"@-ÖVöÄVæ&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†ε.I0 x-ævöÄ,
0010210230	13	C0	2A	C0	99	60	40	56	C6	16	96	27	A2	23	62	93	.Ä*Ä" @VE.-'o#b"
0010210240	02	0B	80	AE	60	10	53	83	93	23	03	03	73	03	43	A7	..e@`.Sf"#.s.CS
0010210250	74	30	86	96	06	67	55	26	37	97	F6	06	06	A1	20	E3	t0+-.gU&7-ö..i ä
0010210260	22	43	23	C2	22	32	C6	F6	36	B6	F6	D5	5F	20	C3	86	"C#Ä"2Eö6qöÖ_ Ä†

Router CALIX 844E-1

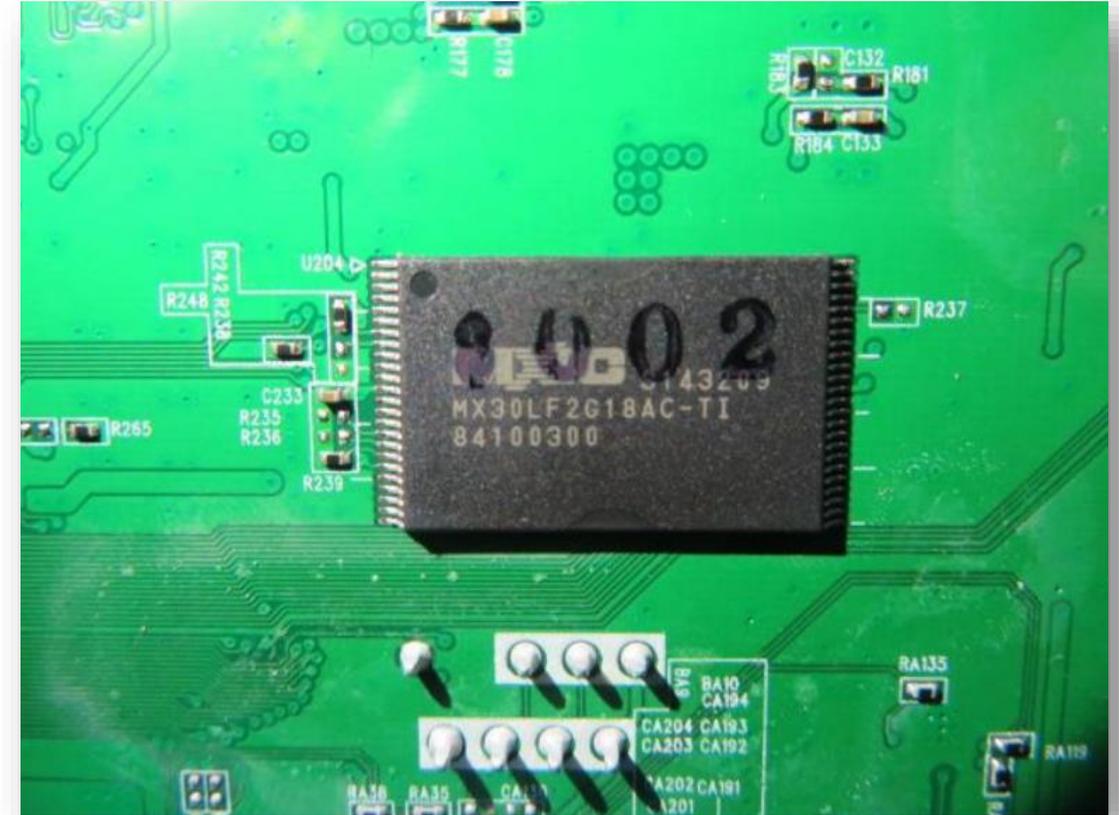
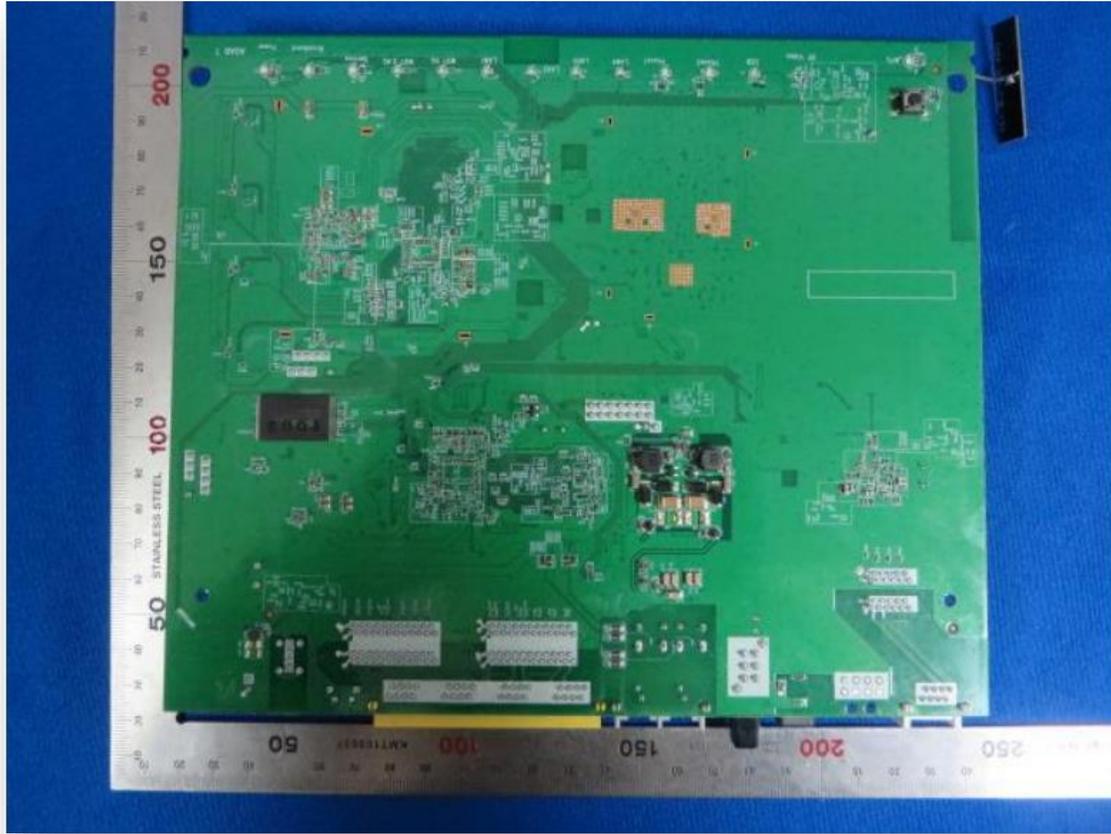


Admin panel



In this case forensic expert had **no login credentials** for the seized device

Electronic board and memory chip (TSOP48)



The device was disassembled to get access to the **data in the memory chip**

NAND memory reading

The screenshot shows the Visual NAND Reader interface. The top menu bar includes 'Case', 'Workspace', and 'Plugins'. The 'Workspace' tab is active, displaying a grid of elements. On the left, a 'Reader 0' is connected to four 'Phy image' blocks, each representing a chip: 'Chip0_0_0', 'Chip1_0_0', 'Chip2_0_0', and 'Chip3_0_0'. A red line connects the Reader to the first chip. A progress dialog is open, showing a 15% progress bar and the text 'Reading dump from reader...'. The dialog also displays 'Chip: Chip0', 'Port: 0', and 'Crystal: 0', with a 'Cancel' button.

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

The physical image of the memory was extracted using VNR

The file system reconstruction

Car Forensics Project - UBI/UBIFS Parser

Open file: \\SERVER\fileserver\R&D\IOT\Routers\CALIX 844E-1 Router\834\UBIFS.dmp

Save selected

ruSolut

- UBI Image Sequence 1579346373
 - UBIFS Volume exa_data_
 - Root
 - arc
 - log
 - poe
 - smact_data.json
 - ngx_console_saved
 - running_uptime
 - wlanmgr_log_messages_saved
 - upgrade_log.dat
 - delta_0
 - delta_1
 - scratchpad
 - log_message
 - var_log_128k_mapagent_saved
 - current
 - upgrade
 - previous
 - udhcpd
 - udhcpd.conf
 - udhcpd.leases
 - delta_next
 - var_log_messages_reset_saved
- UBI Image Sequence 1523611876
 - UBIFS Volume no_erase_
 - Root
 - calix
 - sys
 - binned_data
 - panic
 - cpu_low_1_thresh_a.txt
 - system_events_log_1
 - system_events_log
 - wan_conn_if_up.txt
 - birth-certificate.xml

File iNum	Access	Number of links	UID	GID	Size	Date	Name
84	-rw-r--r--	1	0	0	459	04.08.2021 05:47	udhcpd.conf
82	-rw-r--r--	1	0	0	2552	04.08.2021 06:47	udhcpd.leases

```
= Address = | ===== HEX file output (up to 1024 bytes) ===== | ===== ASCII =====  
-----  
0x00000000 | 64 65 63 6C 69 6E 65 5F 66 69 6C 65 20 2F 76 61 | decline_file /va  
0x00000010 | 72 2F 75 64 68 63 70 64 2E 64 65 63 6C 69 6E 65 | r/udhcpd.decline  
0x00000020 | 0A 61 75 74 6F 5F 74 69 6D 65 20 39 30 30 0A 69 | .auto_time 900.i  
0x00000030 | 6E 74 65 72 66 61 63 65 20 62 72 30 0A 73 74 61 | nterface br0.sta  
0x00000040 | 72 74 20 31 39 32 2E 31 36 38 2E 32 35 30 2E 31 | rt 192.168.250.1  
0x00000050 | 30 0A 65 6E 64 20 31 39 32 2E 31 36 38 2E 32 35 | 0.end 192.168.25  
0x00000060 | 30 2E 32 30 0A 6F 70 74 69 6F 6E 20 6C 65 61 | 0.200.option lea  
0x00000070 | 73 65 20 38 36 34 30 30 0A 6D 69 6E 5F 6C 65 61 | se 86400.min_lea  
0x00000080 | 73 65 20 33 30 0A 6F 70 74 69 6F 6E 20 73 75 62 | se 30.option sub  
0x00000090 | 6E 65 74 20 32 35 35 2E 32 35 35 2E 32 35 35 2E | net 255.255.255.  
0x000000A0 | 30 0A 6F 70 74 69 6F 6E 20 72 6F 75 74 65 72 20 | 0.option router  
0x000000B0 | 31 39 32 2E 31 36 38 2E 32 35 30 2E 31 0A 6F 70 | 192.168.250.1.op  
0x000000C0 | 74 69 6F 6E 20 64 6E 73 20 31 39 32 2E 31 36 38 | tion dns 192.168  
0x000000D0 | 2E 32 35 30 2E 31 0A 6F 70 74 69 6F 6E 20 64 6E | .250.1.option dn  
0x000000E0 | 73 20 31 39 32 2E 31 36 38 2E 32 35 30 2E 31 0A | s 192.168.250.1.  
0x000000F0 | 6F 70 74 69 6F 6E 20 64 6F 6D 61 69 6E 20 48 6F | option domain Ho  
0x00000100 | 6D 65 0A 69 6E 74 65 72 66 61 63 65 20 62 72 71 | me.interface brq  
0x00000110 | 74 0A 73 74 61 72 74 20 31 36 39 2E 32 35 34 2E | t.start 169.254.  
0x00000120 | 31 2E 32 0A 65 6E 64 20 31 36 39 2E 32 35 34 2E | 1.2.end 169.254.  
0x00000130 | 31 2E 32 0A 6F 70 74 69 6F 6E 20 6C 65 61 73 65 | 1.2.option lease  
0x00000140 | 20 38 36 34 30 30 0A 6D 69 6E 5F 6C 65 61 73 65 | 86400.min_lease  
0x00000150 | 20 33 30 0A 6F 70 74 69 6F 6E 20 73 75 62 6E 65 | 30.option subne  
0x00000160 | 74 20 32 35 35 2E 32 35 35 2E 32 35 35 2E 30 0A | t 255.255.255.0.  
0x00000170 | 6F 70 74 69 6F 6E 20 72 6F 75 74 65 72 20 31 36 | option router 16  
0x00000180 | 39 2E 32 35 34 2E 31 2E 31 0A 6F 70 74 69 6F 6E | 9.254.1.1.option  
0x00000190 | 20 64 6E 73 20 31 36 39 2E 32 35 34 2E 31 2E 31 | dns 169.254.1.1  
0x000001A0 | 0A 6F 70 74 69 6F 6E 20 64 6E 73 20 31 36 39 2E | .option dns 169.  
0x000001B0 | 32 35 34 2E 31 2E 31 0A 6F 70 74 69 6F 6E 20 64 | 254.1.1.option d  
0x000001C0 | 6F 6D 61 69 6E 20 48 6F 6D 65 0A | omain Home.
```

A very interesting files with DHCP lease log and config were found.
It can give an idea when the specific device was last seen in the network.


```
system_events_log x
122 2020/08/03|09:56:54|CXNK006B3CE8|421905047719|12.2.9.8.11|Event_NORMAL|wlanmgr|power_off-qtn-device|
123 2020/08/03|09:58:19|CXNK006B3CE8|421905047719|12.2.9.8.11|Critical|wlanmgr|QUANTENNA_LOADER_PING_FAILED_REBOOT_QTN|
124 2020/08/03|09:58:20|CXNK006B3CE8|421905047719|12.2.9.8.11|Critical|wlanmgr|QUANTENNA_RESTART_FIRMWARE_LOAD_FAILED_REBOOT_QTN|
125 2020/08/03|09:58:20|CXNK006B3CE8|421905047719|12.2.9.8.11|Event_NORMAL|wlanmgr|power_off-qtn-device|
126 2020/08/03|09:59:48|CXNK006B3CE8|421905047719|12.2.9.8.11|Critical|wlanmgr|QUANTENNA_LOADER_PING_FAILED_REBOOT_QTN|
127 2020/08/03|09:59:48|CXNK006B3CE8|421905047719|12.2.9.8.11|Critical|wlanmgr|QUANTENNA_RESTART_FIRMWARE_LOAD_FAILED_REBOOT_QTN|
128 2020/08/03|09:59:48|CXNK006B3CE8|421905047719|12.2.9.8.11|Event_NORMAL|wlanmgr|power_off-qtn-device|
129 2020/08/03|10:01:14|CXNK006B3CE8|421905047719|12.2.9.8.11|Critical|wlanmgr|QUANTENNA_LOADER_PING_FAILED_REBOOT_QTN|
130 2020/08/03|10:01:15|CXNK006B3CE8|421905047719|12.2.9.8.11|Critical|wlanmgr|QUANTENNA_RESTART_FIRMWARE_LOAD_FAILED_REBOOT_QTN|
131 2020/08/03|10:01:15|CXNK006B3CE8|421905047719|12.2.9.8.11|Event_NORMAL|wlanmgr|power_off-qtn-device|
132 1969/12/31|20:00:34|CXNK006B3CE8|421905047719|12.2.9.8.11|Event_NORMAL|healthmgr|WAN's wanIfNames initialized to eth5|
133 1969/12/31|20:00:34|CXNK006B3CE8|421905047719|12.2.9.8.11|Event_NORMAL|healthmgr|Cold boot flag set, possible power up restart|
134 1969/12/31|19:01:42|CXNK006B3CE8|421905047719|12.2.9.8.11|Event_NORMAL|smd|fail_2rd_collect_upnp_2577|
135 1969/12/31|19:02:20|CXNK006B3CE8|421905047719|12.2.9.8.11|Critical|healthmgr|resource mon: Halfway to cpu LOW Threshold|
136 1969/12/31|19:03:47|CXNK006B3CE8|421905047719|12.2.9.8.11|Critical|healthmgr|resource mon: LOW cpu State active|
137 1969/12/31|20:41:24|CXNK006B3CE8|421905047719|12.2.9.8.11|Critical|wlanmgr|QUANTENNA_INIT_FIRMWARE_LOAD_FAILED_REBOOT_QTN|
138 1969/12/31|20:41:25|CXNK006B3CE8|421905047719|12.2.9.8.11|Event_NORMAL|wlanmgr|power_off-qtn-device|
139 1969/12/31|19:00:34|CXNK006B3CE8|421905047719|12.2.9.8.11|Event_NORMAL|healthmgr|WAN's wanIfNames initialized to eth5|
140 1969/12/31|19:00:34|CXNK006B3CE8|421905047719|12.2.9.8.11|Event_NORMAL|healthmgr|Cold boot flag set, possible power up restart|
141 1969/12/31|19:01:54|CXNK006B3CE8|421905047719|12.2.9.8.11|Critical|healthmgr|resource mon: Halfway to cpu CRITICAL Thresh|
142 1969/12/31|19:02:20|CXNK006B3CE8|421905047719|12.2.9.8.11|Critical|healthmgr|resource mon: Halfway to cpu LOW Threshold|
143 1969/12/31|19:05:10|CXNK006B3CE8|421905047719|12.2.9.8.11|Critical|healthmgr|resource mon: Halfway to cpu LOW Threshold|
144 1969/12/31|19:09:36|CXNK006B3CE8|421905047719|12.2.9.8.11|Critical|healthmgr|resource mon: Halfway to cpu LOW Threshold|
145 1969/12/31|19:16:54|CXNK006B3CE8|421905047719|12.2.9.8.11|Critical|healthmgr|resource mon: Halfway to cpu LOW Threshold|
146 1969/12/31|19:18:26|CXNK006B3CE8|421905047719|12.2.9.8.11|Critical|healthmgr|resource mon: LOW cpu State active|
147 1969/12/31|20:20:45|CXNK006B3CE8|421905047719|12.2.9.8.11|Event_NORMAL|wlanmgr|qtn_client_create_success|
148 2020/08/03|14:18:29|CXNK006B3CE8|421905047719|12.2.9.8.11|Critical|healthmgr|resource mon: Fallback to Normal State.|
149 2020/08/03|14:20:23|CXNK006B3CE8|421905047719|12.2.9.8.11|Event_NORMAL|wlanmgr|QT_HOSTAPD_UP|
150 2020/08/12|16:38:15|CXNK006B3CE8|421905047719|12.2.9.8.11|Event_NORMAL|healthmgr|resource mon: /var/tmp/shmem_usage Err(-4006) 0x0001|
151 1969/12/31|20:00:34|CXNK006B3CE8|421905047719|12.2.9.8.11|Event_NORMAL|healthmgr|WAN's wanIfNames initialized to eth5|
152 1969/12/31|20:00:34|CXNK006B3CE8|421905047719|12.2.9.8.11|Event_NORMAL|healthmgr|Cold boot flag set, possible power up restart|
153 2020/08/13|08:14:40|CXNK006B3CE8|421905047719|12.2.9.8.11|Event_NORMAL|wlanmgr|qtn_client_create_success|
154 2020/08/13|08:17:08|CXNK006B3CE8|421905047719|12.2.9.8.11|Event_NORMAL|wlanmgr|QT_HOSTAPD_UP|
155 2020/08/17|02:15:54|CXNK006B3CE8|421905047719|12.2.9.8.11|Event_NORMAL|healthmgr|resource mon: /var/tmp/shmem_usage Err(-4006) 0x0001|
```

Some additional event data can be extracted from the System and CPU logs.

Wearables are everywhere. A first look into Huawei GT2 smartwatch



Sensor set

GPS

Bluetooth

Accelerometer sensor

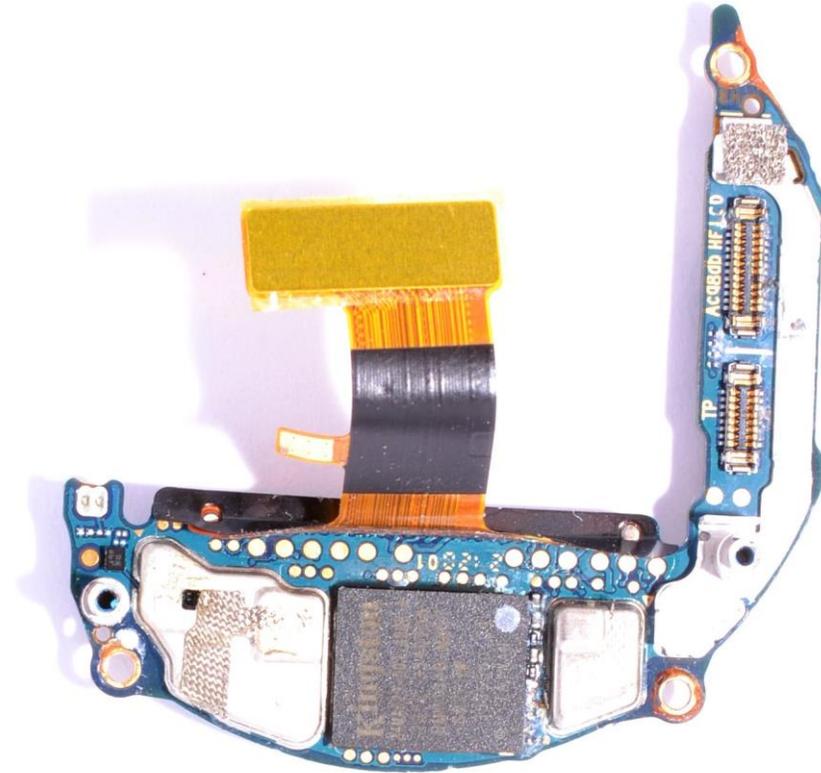
Gyroscope sensor

Geomagnetic sensor

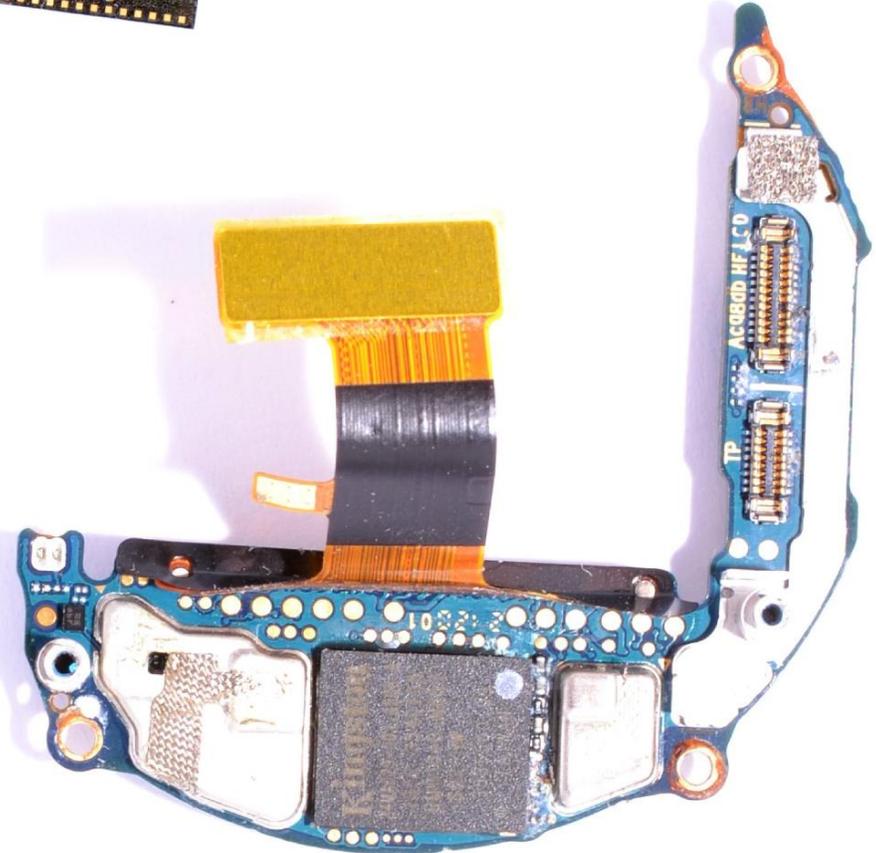
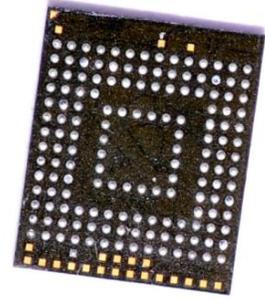
Optical heart rate sensor

Ambient light sensor

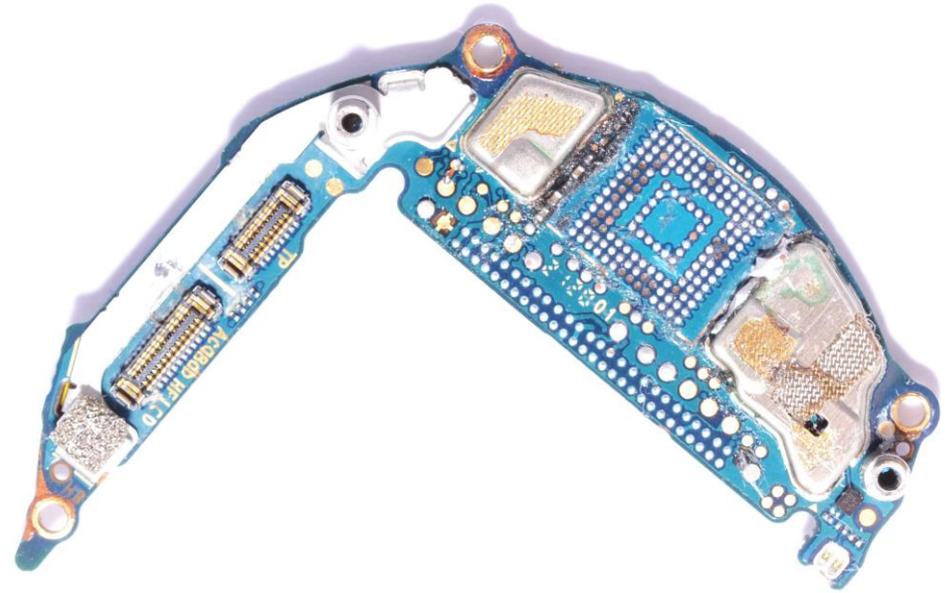
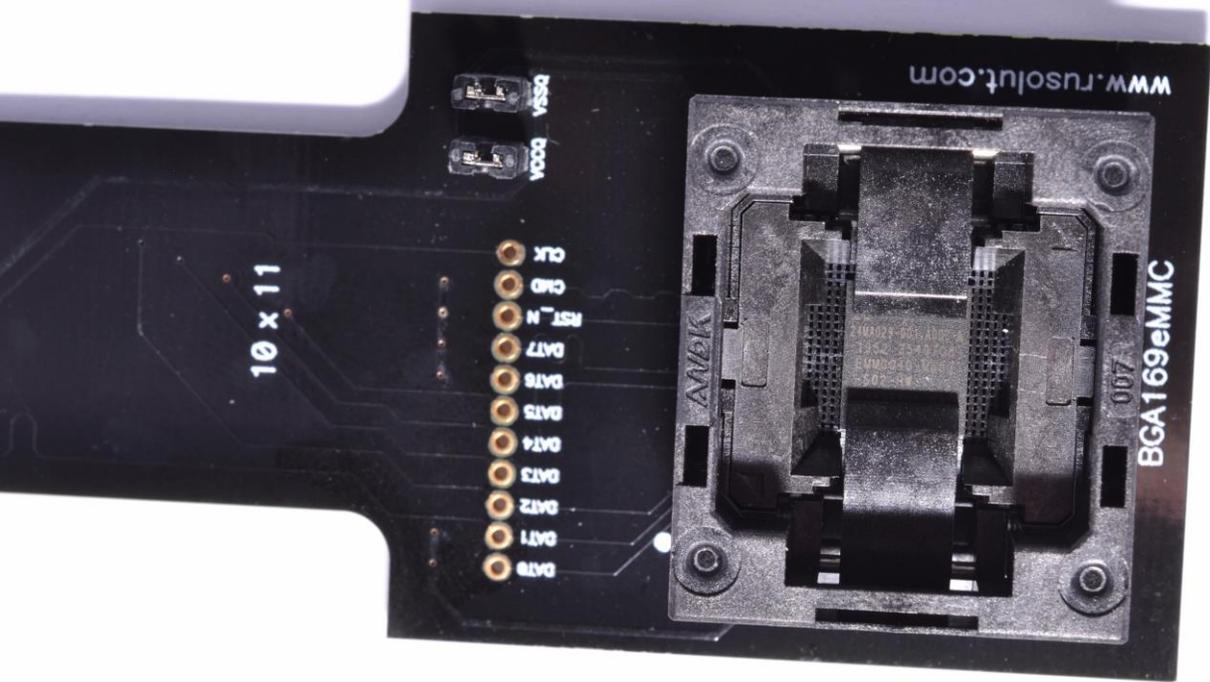
Air pressure sensor



The eMMC memory chip with 4GB of space!



The eMMC chip is smaller than smallest one we have adapter for



The memory had to be precisely adjusted inside the adapter for the image extraction, since only size differs but not pinout

The file system structure – multiple FAT32 volumes

The screenshot displays a forensic analysis tool interface with three main panes:

- Left Pane (File System Structure):** Shows a tree view of the file system. The path is MBR > Volume1 (Microsoft FAT32) NO NAME 393.75 MB > Root > USER > LOG. The 'LOG' folder is selected, showing a list of log files such as boot_debug, gpu_debug, GPU_DUMP, GPU_FS, gpu_power, gpu_event, GPU_ERROR, m3dsp_debug, M3_ERROR, mcu_debug, MCU_DUMP, mcu_error, mcu_event, mcu_power, and mcu_safety.
- Middle Pane (Hex Viewer):** Displays hex data in a grid format. The address 421017600 is selected. The data shows a sequence of bytes representing a boot log entry.
- Right Pane (Text Viewer):** Shows the ASCII representation of the hex data. It contains a boot log entry with the following text:

```
[1999] [bsp] [INFO] INIT:boot build date:*** Feb 6 2020 ***.[1999] [bsp] [INFO] INIT:boot build time:*** 11:16:57 ***.[1999] [bsp] [INFO] INIT:boot build version:*** 1.0.0.3 ***.[116594] [bsp] [ERROR] file close err..[378602] [boot] [INFO] === update success ===.[1877] [bsp] [INFO] INIT:boot build date:*** Apr 10 2020 ***.[1877] [bsp] [INFO] INIT:boot build time:*** 23:10:22 ***.[1877] [bsp] [INFO] INIT:boot build version:*** 1.0.0.3 ***.[306755] [boot] [ERROR]
```

At the bottom of the tool, there is an 'Event log explorer' pane and a status bar showing 'Record start: 413321856', 'Data start: 421017600', and 'Address: 421017600 Selected: 0'.

Quick analysis shows lots of **logs** of smartwatch boot and usage

Data storage folder was identified

Visual Nand Reconstructor - Huawei_Watch_GT2_LTN_B19

Case Navigator Hex viewer

Hex view Bitmap view Structure view Records view Save all Save selected Extract selected to workspace Frame view Frame size: 512 Current frame: 827660 / 7405567 Show structure View settings

Copy 0 X Workspace Copy 0 X

MBR Volume1 (Microsoft FAT32) NO NAME 393.75 MB Root USER DATA HEALTH

MBR Volume0 (Microsoft FAT32) NO NAME 393.72 MB Volume1 (Microsoft FAT32) NO NAME 393.75 MB Root USER ALBUM BUSCARDS CONFIG DATA HEALTH GPS LOG MARKET RES TEST FAT0 FSInfo Volume2 (Microsoft FAT32) NO NAME 287.44 MB Volume3 (Microsoft FAT32) NO NAME 2.47 GB

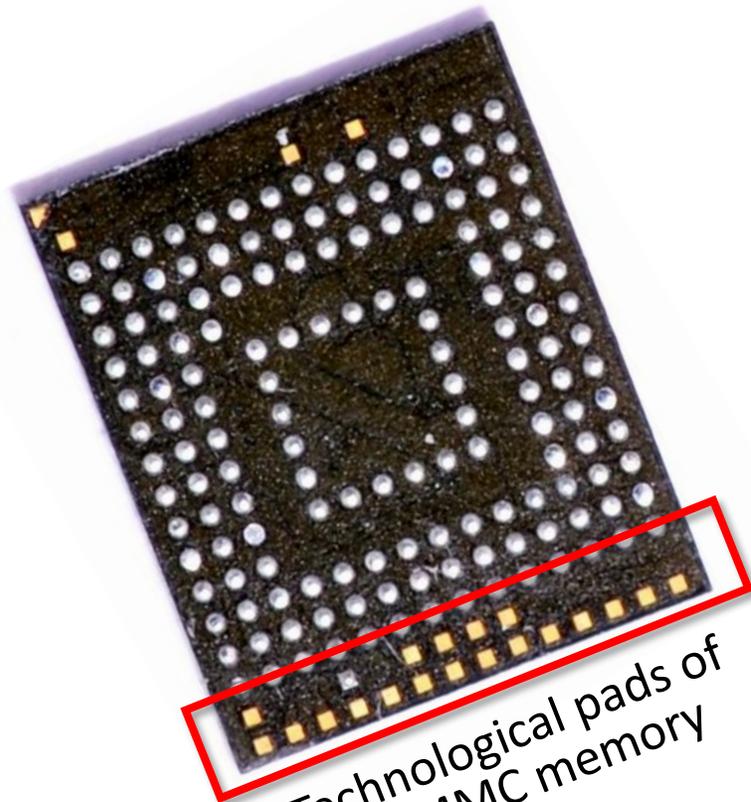
Name	Ext	Size	Last modified
..			
atrial_data	bin	316 bytes	01/01/1980 00:00:00
ete_for_tha	bin	0 bytes	01/01/1980 00:00:00
ete_for_tha_file	bin	8 bytes	01/01/1980 00:00:00
ete_result	bin	0 bytes	01/01/1980 00:00:00
hrm_adaptparamdata	bin	146 bytes	01/01/1980 00:00:00
hrm_fallreminddata	bin	3.99 KB	01/01/1980 00:00:00
hrm_historydata	bin	126 bytes	01/01/1980 00:00:00
hrm_raisereminddata	bin	3.99 KB	01/01/1980 00:00:00
motion_data	bin	28.39 KB	01/01/1980 00:00:00
osa_rri_data	bin	0 bytes	01/01/1980 00:00:00
osa_spo2_data	bin	0 bytes	01/01/1980 00:00:00
premature_data	bin	316 bytes	01/01/1980 00:00:00
pressure_altitude	bin	640 bytes	01/01/1980 00:00:00
pressure_warn	bin	432 bytes	01/01/1980 00:00:00
RRR_DATA	BIN	0 bytes	01/01/1980 00:00:00
sample_data	bin	289.00 KB	01/01/1980 00:00:00
sample_data_file	bin	8 bytes	01/01/1980 00:00:00
sample_state	bin	128.25 KB	01/01/1980 00:00:00
sample_state_file	bin	8 bytes	01/01/1980 00:00:00
sleep_data	bin	704.00 KB	01/01/1980 00:00:00
sleep_data_file	bin	8 bytes	01/01/1980 00:00:00
sleep_state	bin	60.00 KB	01/01/1980 00:00:00
sleep_state_file	bin	8 bytes	01/01/1980 00:00:00
SPO2	BIN	0 bytes	01/01/1980 00:00:00
spo2_file	bin	8 bytes	01/01/1980 00:00:00
strength_data	bin	47.44 KB	01/01/1980 00:00:00
stress_data	bin	0 bytes	01/01/1980 00:00:00
stress_data_file	bin	4 bytes	01/01/1980 00:00:00
stress_ui_data	bin	484 bytes	01/01/1980 00:00:00
SWIMHR	BIN	0 bytes	01/01/1980 00:00:00
swimhr_file	bin	8 bytes	01/01/1980 00:00:00
swim_section	bin	0 bytes	01/01/1980 00:00:00
swim_section_file	bin	8 bytes	01/01/1980 00:00:00
workout_detail	bin	1024 bytes	01/01/1980 00:00:00
workout_detail_curve	bin	0 bytes	01/01/1980 00:00:00
workout_detail_curve_file	bin	8 bytes	01/01/1980 00:00:00

```
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
0019421800 00 00 00 00 23 B9 E2 62 00 00 64 01 10 00 01 01
0019421810 51 E6 42 B1 54 03 36 A8 12 24 08 50 51 40 62 4E
0019421820 F1 5F 44 61 2E 4A 0F 14 2A 50 99 8B 1B C7 D1 A7
0019421830 9D 38 60 14 45 F0 0F 4C 35 D1 1F D2 50 EB 7A 2E
0019421840 B5 13 D9 CF 52 87 FE 38 0E 5E 6B 71 D6 DC CD 95
0019421850 26 FC A7 5C DA 26 52 18 2C 45 EC 09 EC 47 A2 56
0019421860 15 46 E2 7A DA 70 29 8B DC 02 FC 79 4E A4 11 E7
0019421870 BD 5A BA F4 6F 95 B5 C0 0D FD 0A 91 3C A8 6E 43
0019421880 81 09 ED 74 D2 F5 A2 15 84 5D 58 32 B8 69 E1 09
0019421890 BF 7F CE 97 5A 03 2F EF 2C 07 34 2B D5 62 AC FC
00194218A0 1C 80 64 F6 D2 78 01 F5 E2 6B FA 02 ED 5C D6 95
00194218B0 9C 15 C5 B1 09 D7 16 99 FC 4A FF 2F 7E 50 46 A7
00194218C0 37 FC 01 03 30 BA E2 A0 BA DA 2D 66 06 FB 52 47
00194218D0 23 92 E3 DD 10 77 82 05 E2 B4 61 30 F0 84 FA 5F
00194218E0 2D 5C 1B 10 EA 81 C6 93 54 20 3B 5C 82 D0 01 41
00194218F0 7C 48 02 96 C0 CE C1 C0 1F 2E 4F 5D 4D 0E 03 82
0019421900 14 EB F6 12 47 5F 0D D0 82 38 4A F3 78 A0 6C 78
0019421910 5E 43 07 A7 F4 A4 A9 6A 36 5E 7F 15 45 45 04 97
0019421920 50 79 1A F7 FD 91 8D 03 2A 1B 96 11 BC 50 8A EE
0019421930 73 2A 90 01 0E E7 A7 42 A5 12 02 2B 06 54 A5 47
0019421940 01 61 53 78 73 77 99 AF E1 48 48 B7 11 9A 80 AE
0019421950 71 C7 4D D0 53 60 4E D5 2F 4C B0 B2 F4 66 91 8B
0019421960 D5 EB 68 DE 8C C2 90 E3 33 05 35 8B A4 F4 00 AB
0019421970 56 17 1D 84 81 09 84 C3 4B AD 7F 9A BA 06 01 82
0019421980 55 E5 4C EC 18 52 C6 AA E2 B8 AD F3 1E 68 3C E7
0019421990 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00194219A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00194219B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00194219C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00194219D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00194219E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00194219F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

...#ab.d....
QeBzT.6...PQ@bN
n_Da.U...P...cNS
0B...E8.L5N.0Pez.
μ.ÜR+þ8.^kqÜÜi+
äú\$UáR,.Ei.iGoV
.FázÜp)Ü.üyNR.ç
%Z°ðo•pÄ.ý.<'nC
Q.it0ðo..jX2.iá.
ç I-z./i..4+0b-ü
.eq00x.0ákú.i\0
e.Ä±.x.üJy/~PF\$
7ü..0°á °Ü-f.ÜRG
#'áY.w..á'a0ð.ú_
-\..éÜE" T ;\,D.A
|H.-ÄIÄÄ..0JM..,
.eð.G..ð.8JÜx lx
^C.gðw@j6^ .EE.-
Py.-ý'Q.+. -4P\$Í
s*Q..ç\$Bÿ..+TYG
.asxsw" äHH-.3e@
qçMps_N0/L*"0f'k
ÖehpGÄÜg3.5<0ð.«
V...Q..ÄK. s°...
UäLi.RE*Ä..ö.h<ç

Further analysis is required to pull out the readable data

Historical data access can be gained via direct NAND reading



Technological pads of the eMMC memory

It's almost IMPOSSIBLE to wipe out the data from eMMC chips, most of devices keep erased data for an indefinite time. Connection to technological NAND pads of eMMC memory is required to recover all the artefacts of the user's data. The **eMMC-NAND Reconstructor** is the tool for handling such tasks.

More information about technology can be found on <https://rusolut.com/emmc-nand-reconstructor/>

also in scientific paper published in IEEE <https://ieeexplore.ieee.org/document/9777707>

The screenshot shows the IEEE Xplore website interface. At the top, there's a navigation bar with 'IEEE.org', 'IEEE Xplore', 'IEEE SA', 'IEEE Spectrum', and 'More Sites'. Below that, the 'IEEE Xplore' logo is followed by 'Browse', 'My Settings', and 'Help' menus, and an 'Institutional Sign In' button. A search bar with 'All' is visible. The main content area shows the article title 'Experimental Evaluation of e.MMC Data Recovery' with the publisher 'IEEE'. There are buttons for 'Cite This' and 'PDF'. Below the title, the authors are listed: 'Aya Fukami', 'Sasha Sheremetov', 'Francesco Regazzoni', 'Zeno Geradts', and 'Cees De Laat'. At the bottom, there are two boxes: one showing '2 Cites in Papers' and another showing '327 Full Text Views'.

Thank you!!!
www.rusolut.com

Our partner in India



3RD EYE TECHNO SOLUTIONS PVT. LTD
WWW.3ETS.IN