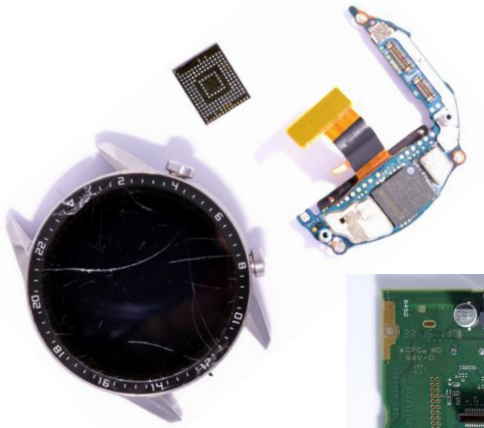
Advanced Forensics
IoT & Vehicle Forensics

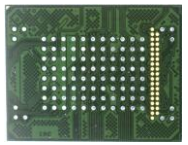
Alexander Sheremetov

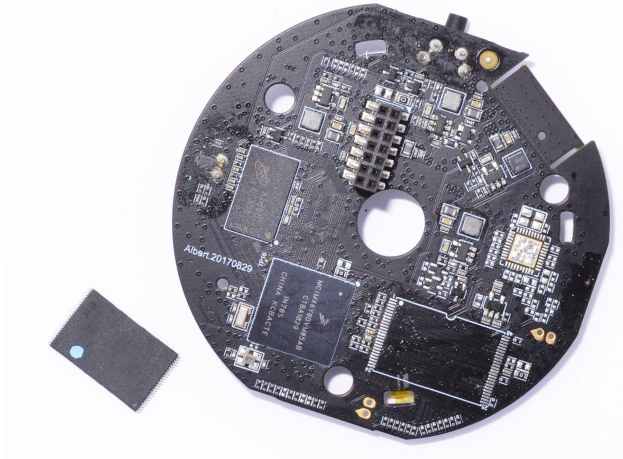
Rusolut, Poland

A New Digital Forensics Era

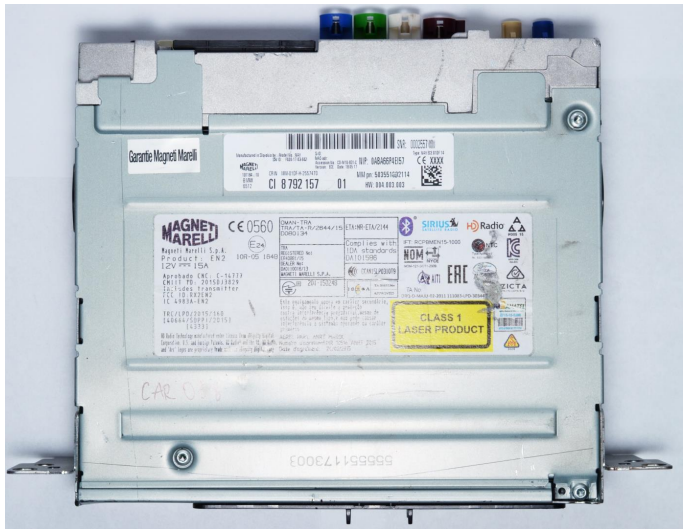
It’s not just mobile forensics anymore.
There are much more data sources than we used to know.
Embedded systems do not always have the interface connectors. Working with the memory chip directly gives a full access to memory and data.

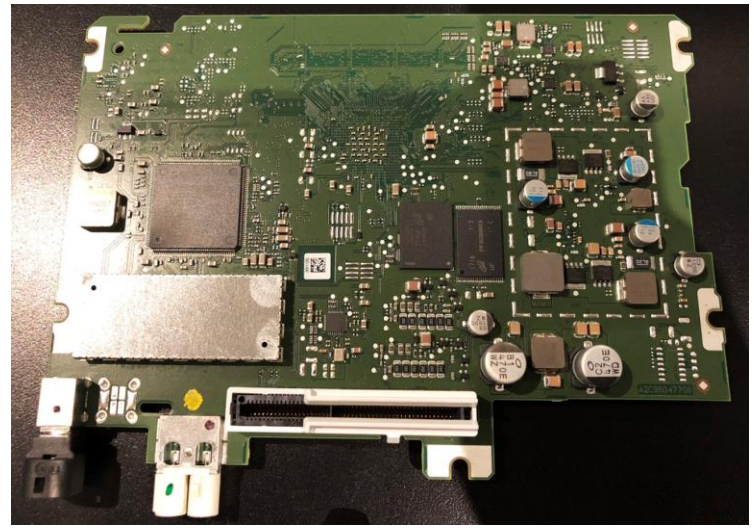






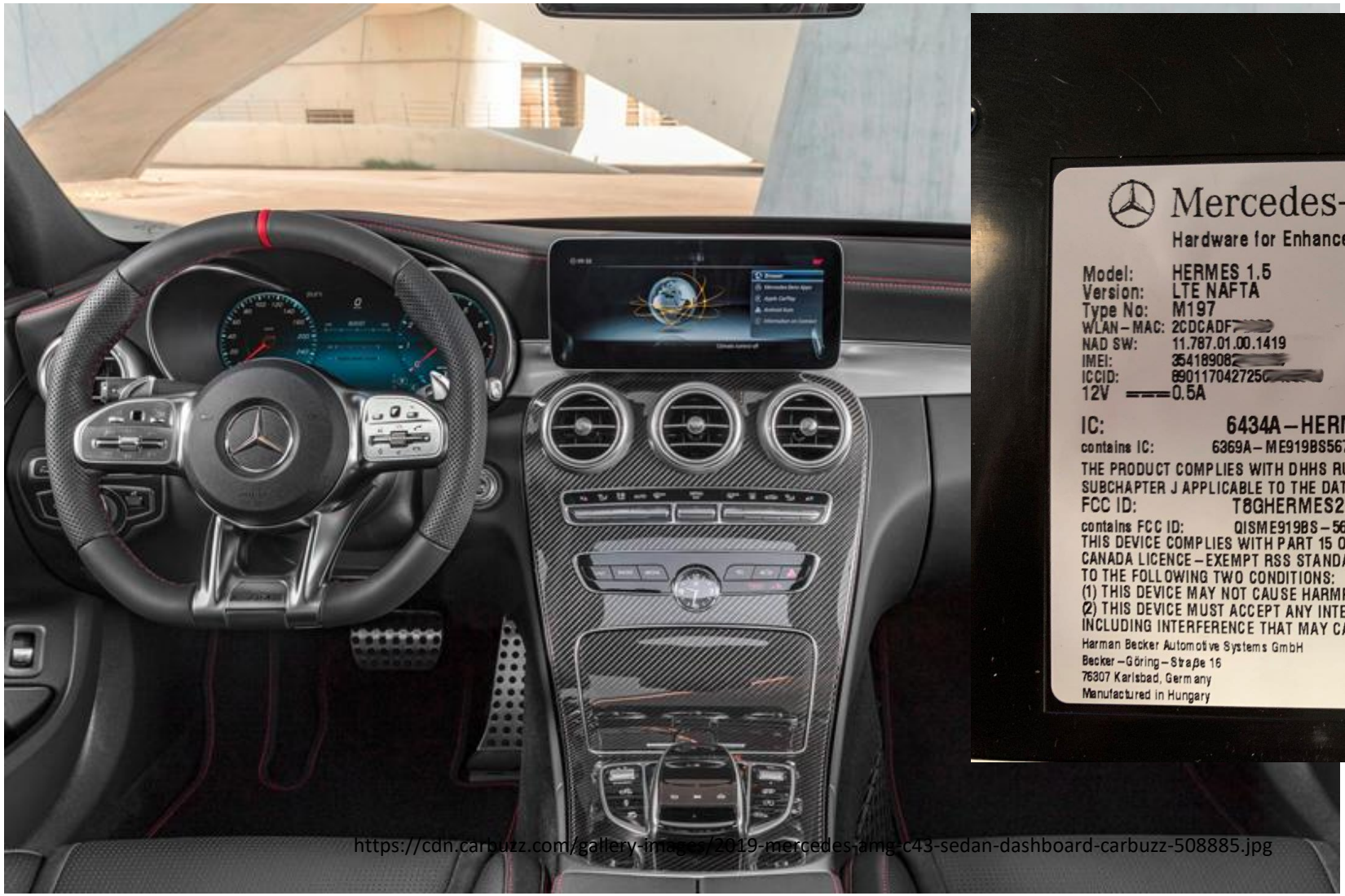
Vehicle forensics – Infotainment systems





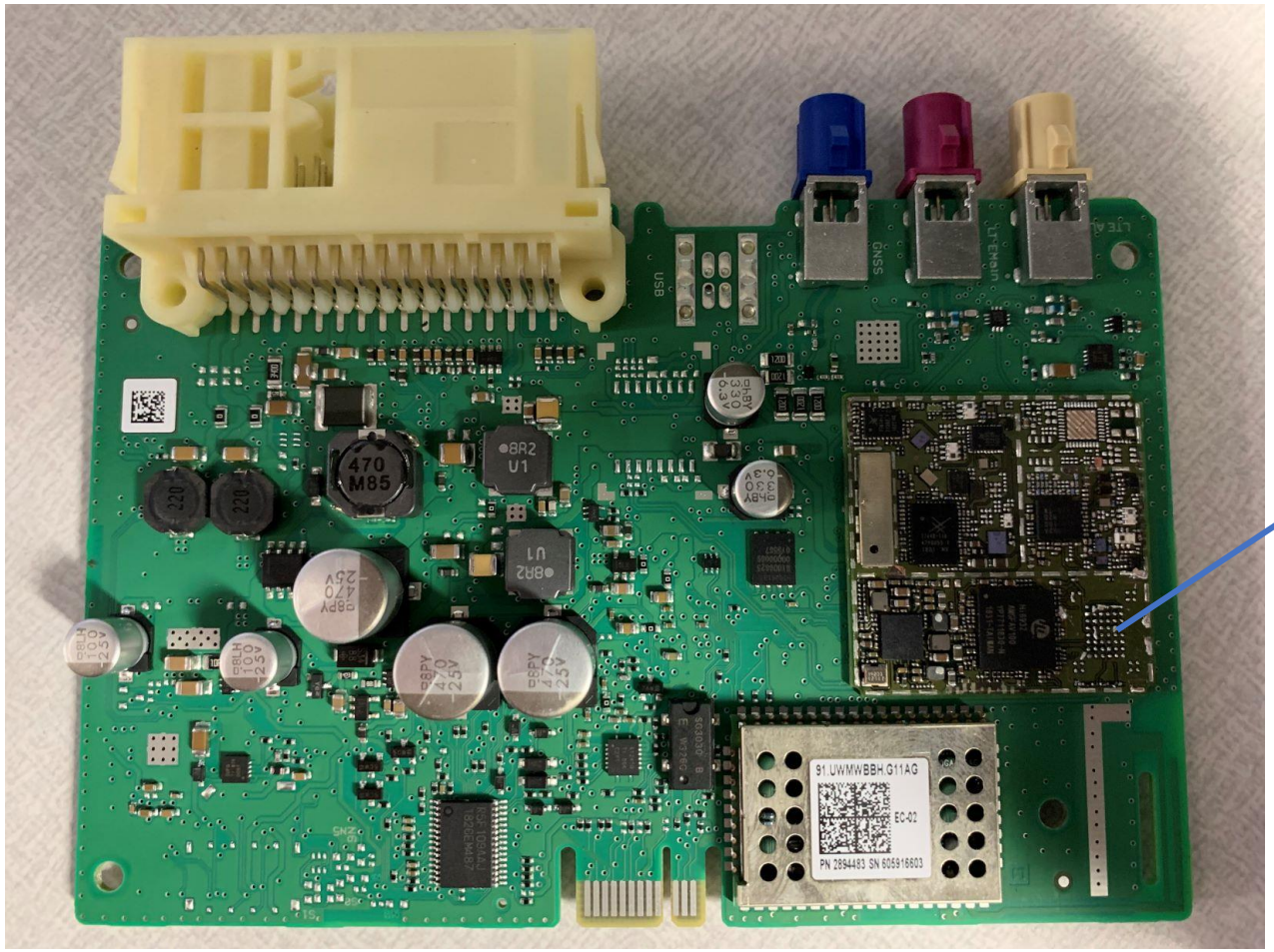
Every modern car has at least one data source, sometimes two or more. The phone normally connects through Bluetooth and lots of data gets synchronized: phone ID data, contact book, call logs, sms, etc. If the system supports GPS, then such data as last destination, trips, fuel data, etc are stored in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

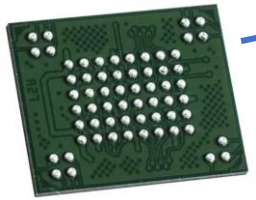
Mercedes AMG C43 - Multimedia Interface Control Unit

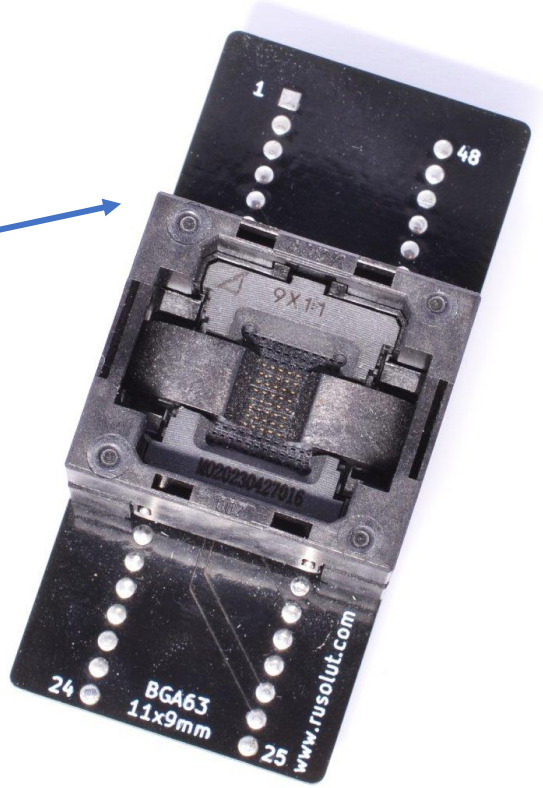


https://cdn.carbuzz.com/gallery-images/2019-mercedes-amg-c43-sedan-dashboard-carbuzz-508885.jpg

Inside Multimedia Interface Control Unit – PCB and memory

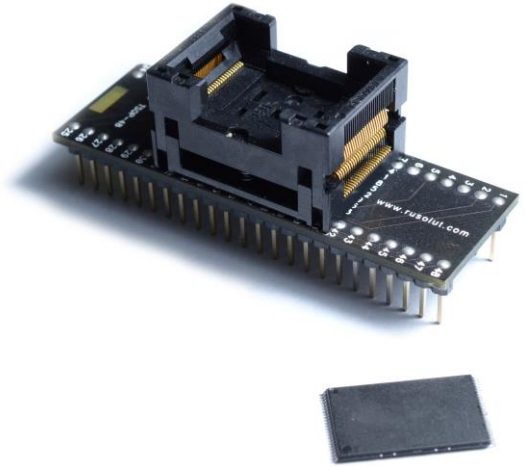


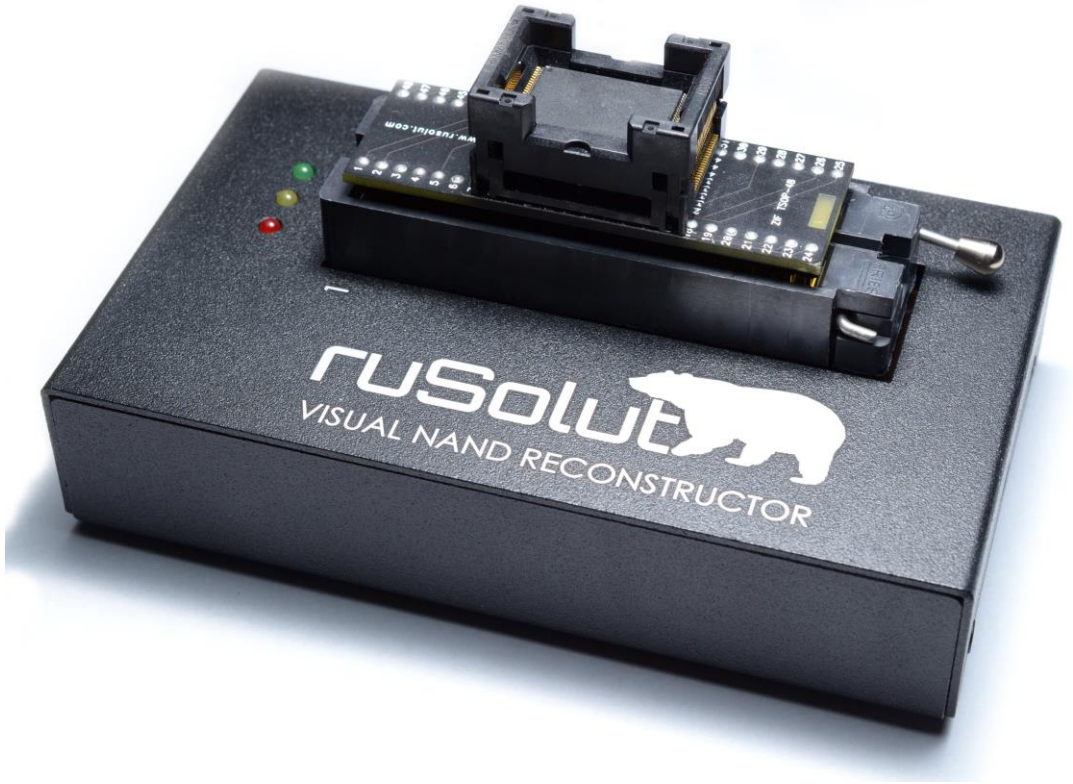




The unit was disassembled and the BGA63 NAND memory chip was extracted using chip-off technique.
The memory chip then was plugged into special BGA63 adapter of Visual NAND Reconstructor.

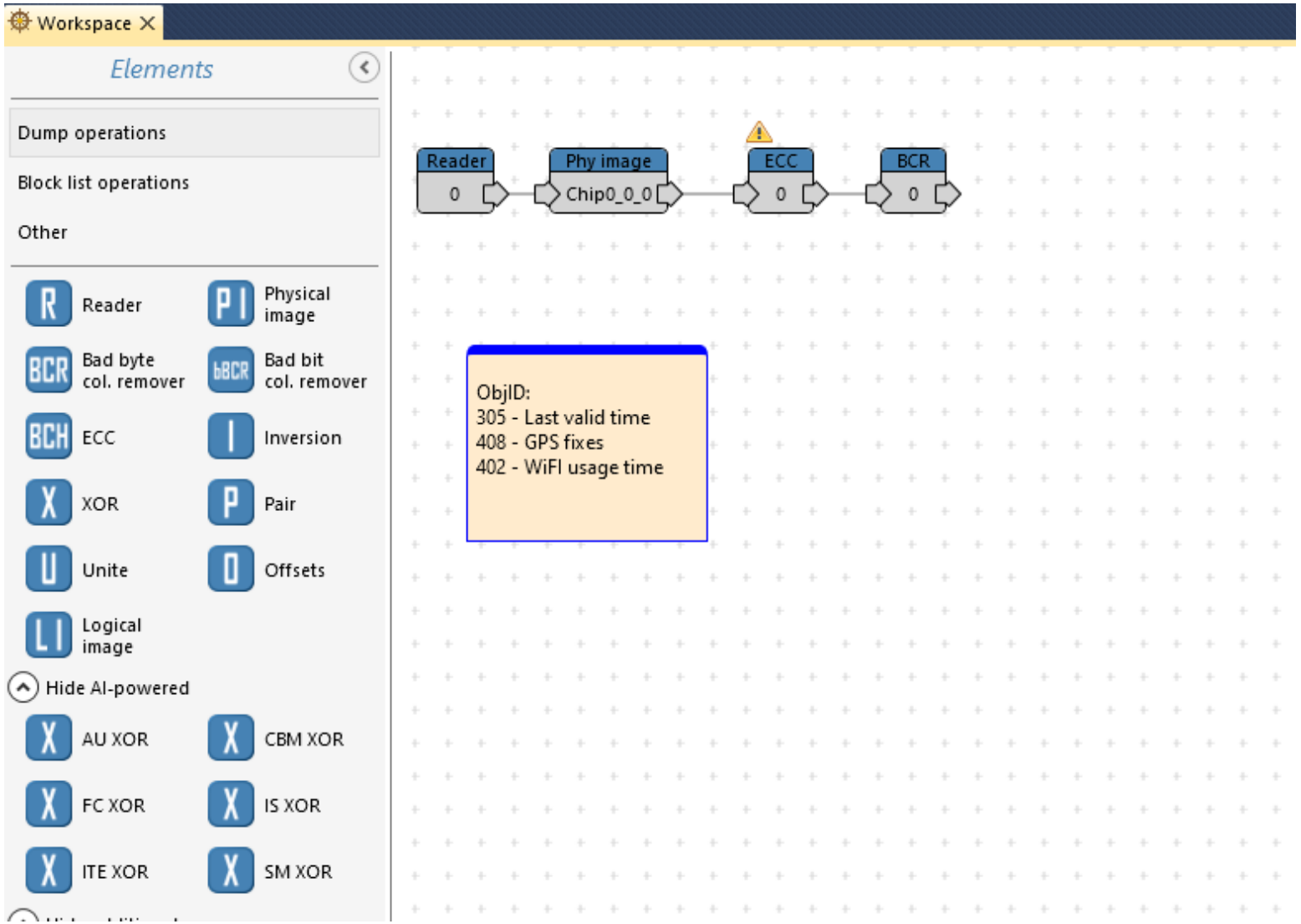
NAND memory in the VNR Reader



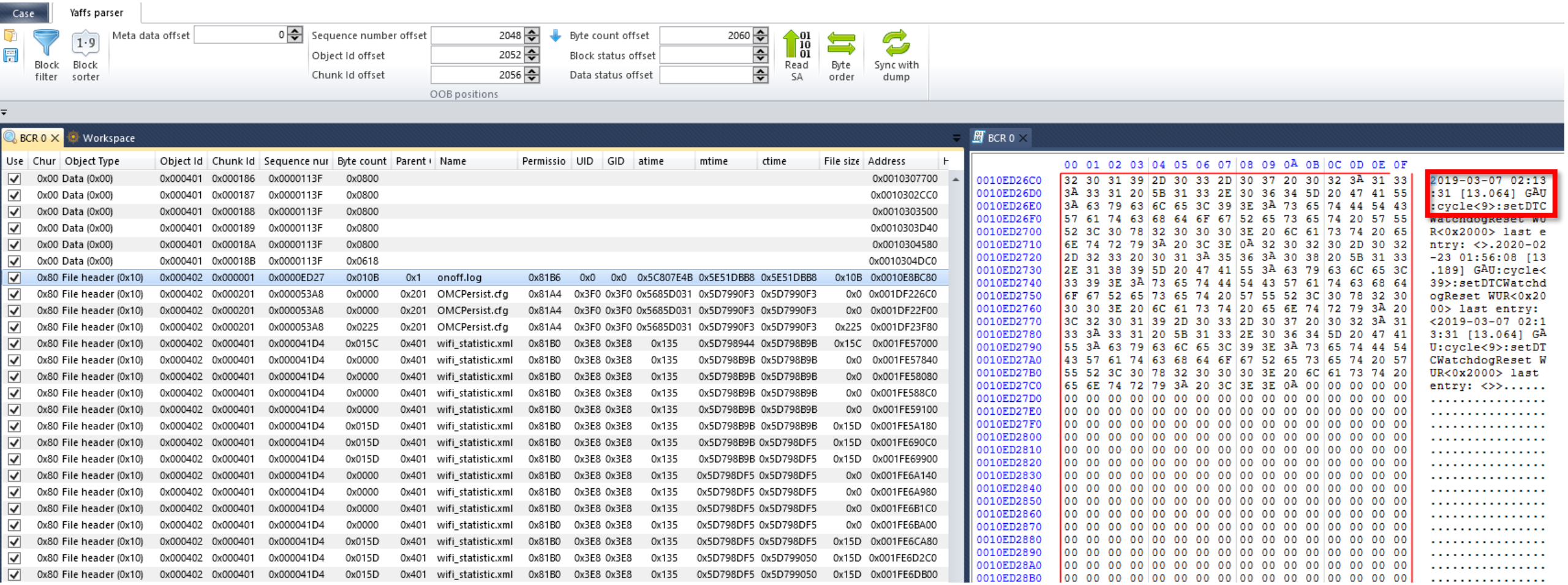


Most of flash memory chips can be read in VNR reader through easy-to-use adapter

NAND memory dump reading and processing



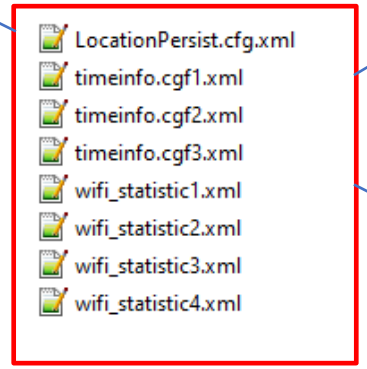
YAFFS2 file system parser – besides user's data, the car's events are also stored for a long time



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
}
```

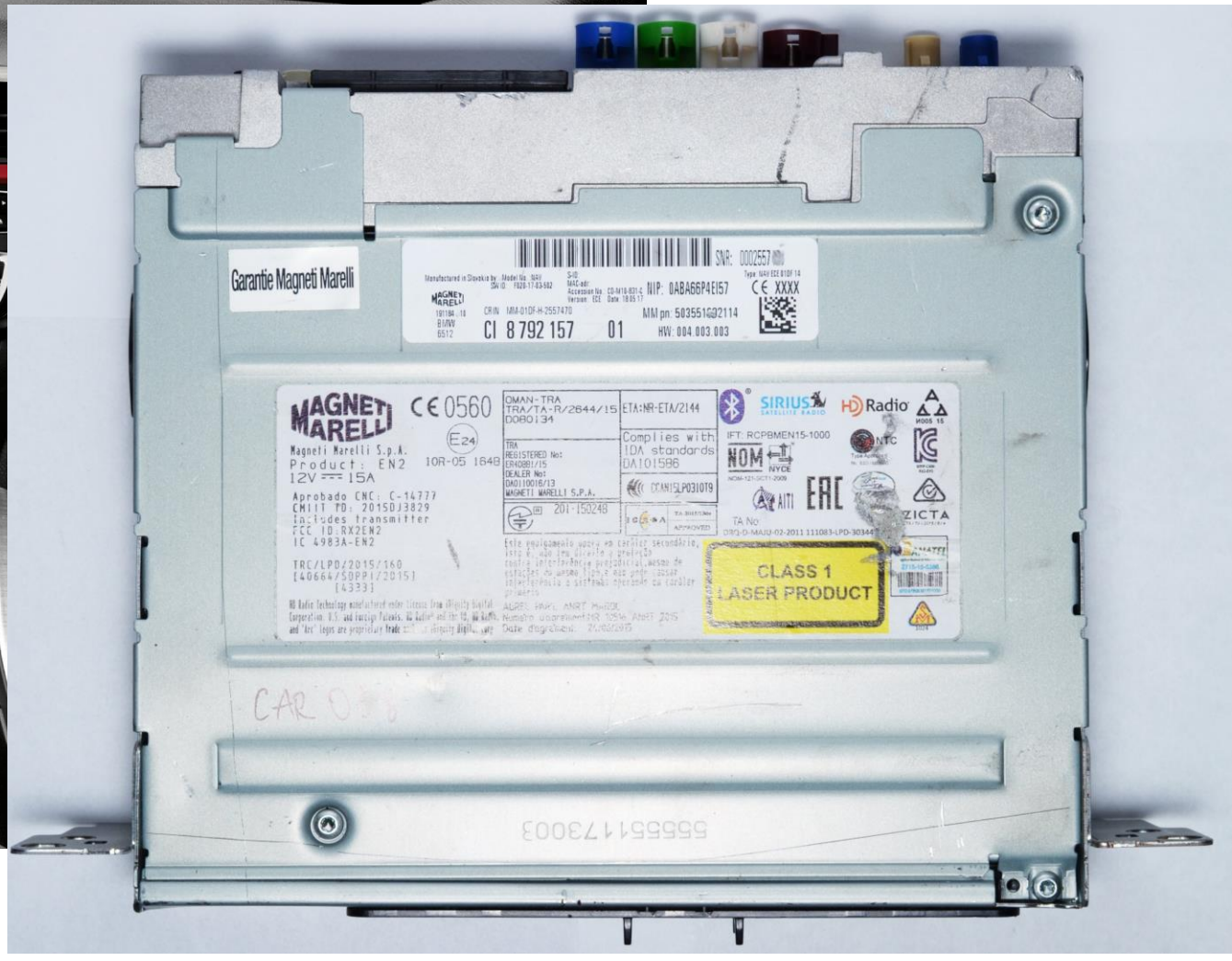
wifi_statistic1.xml

```
<?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>
```

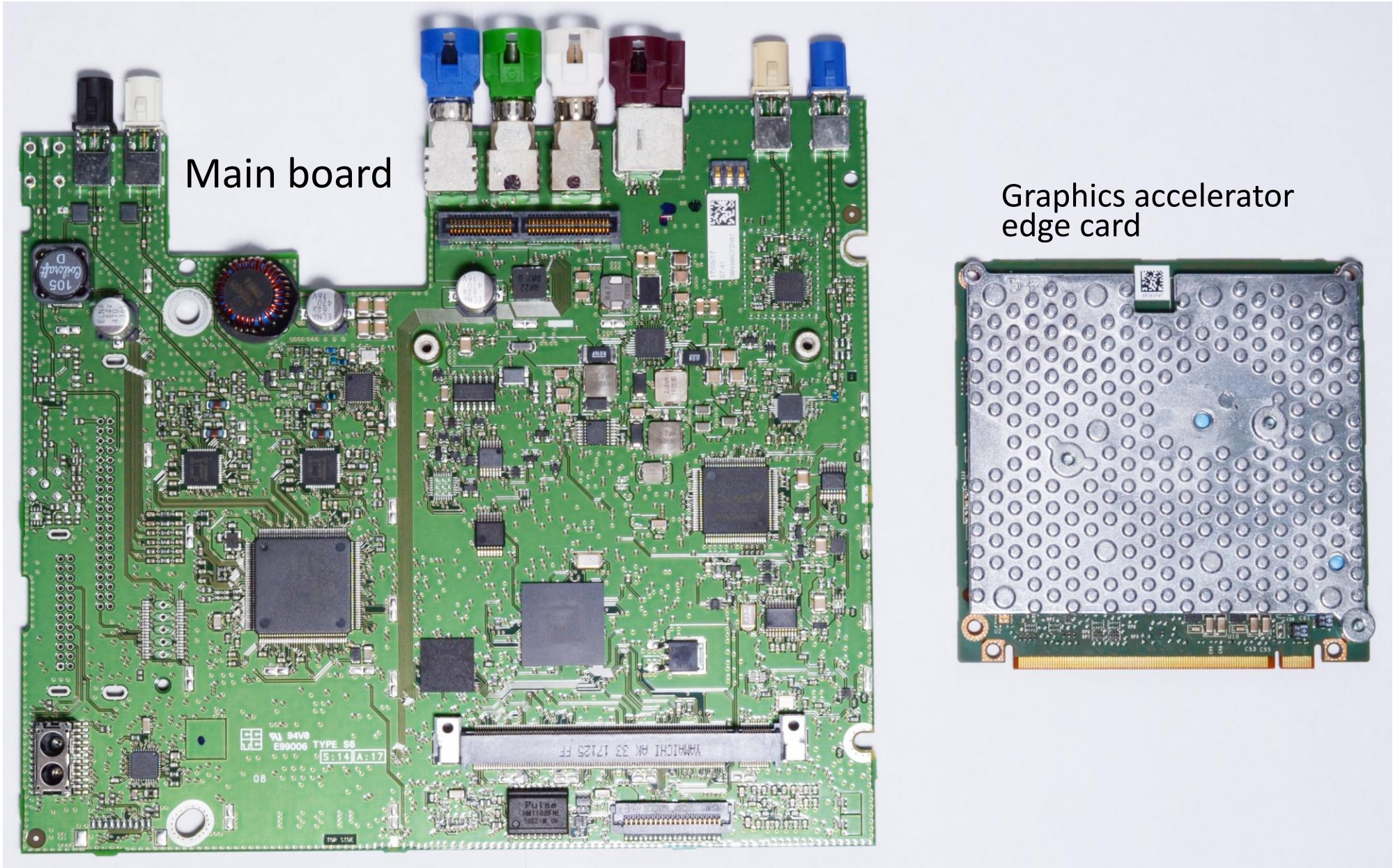
The memory chip holds a vast amount of the navigation data, such as Last destinations with timestamps

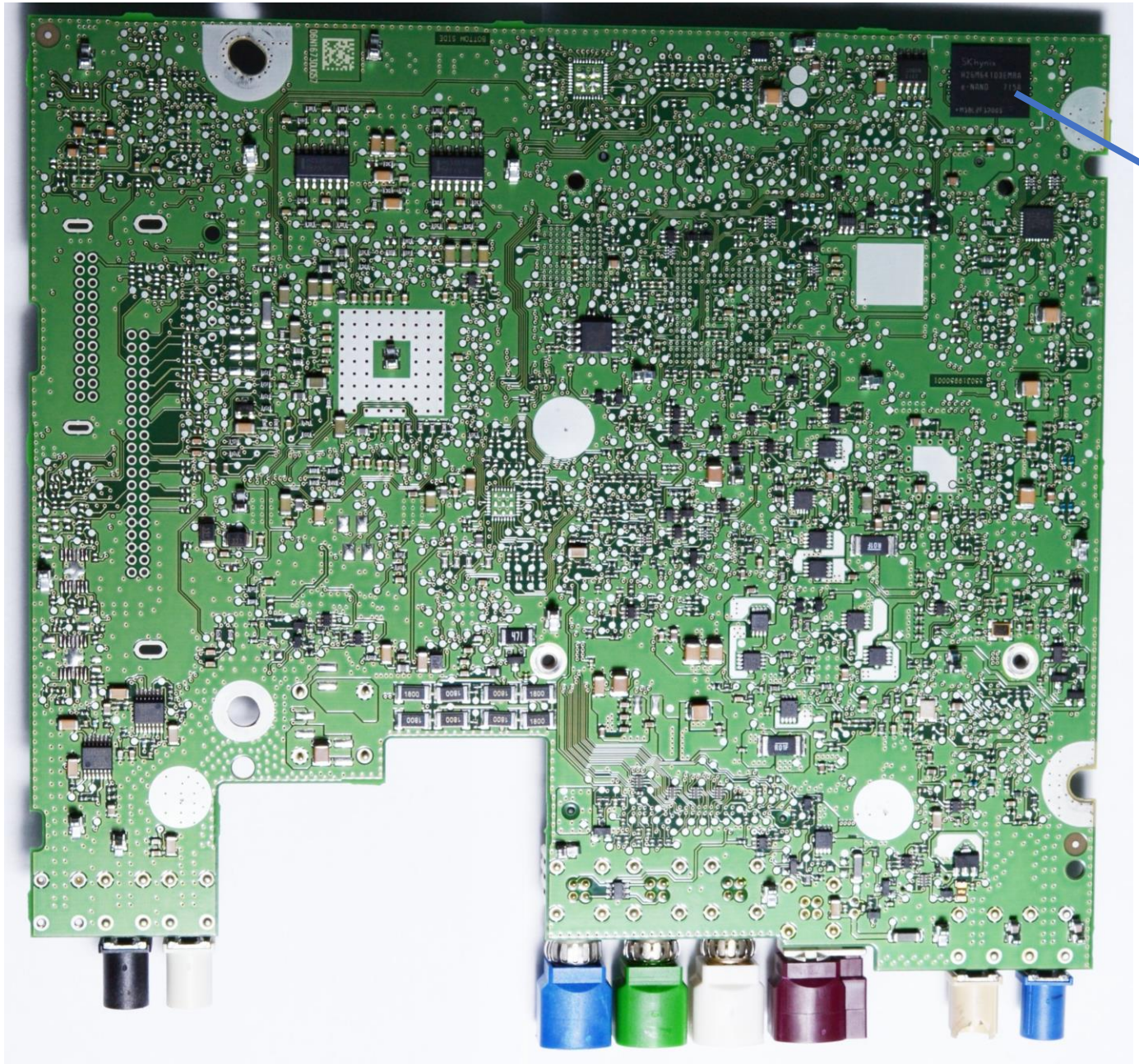
BMW 3 F30 Infotainment system

https://www.carbodydesign.com/gallery/2011/10/the-new-bmw-3-series/2



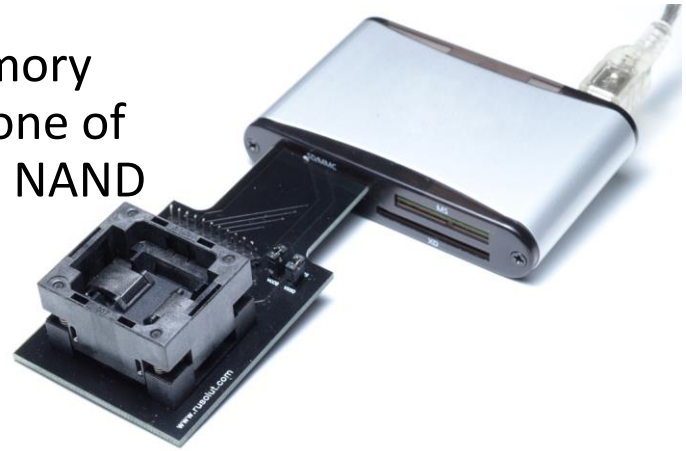
Internal boards extracted from the Infotainment system



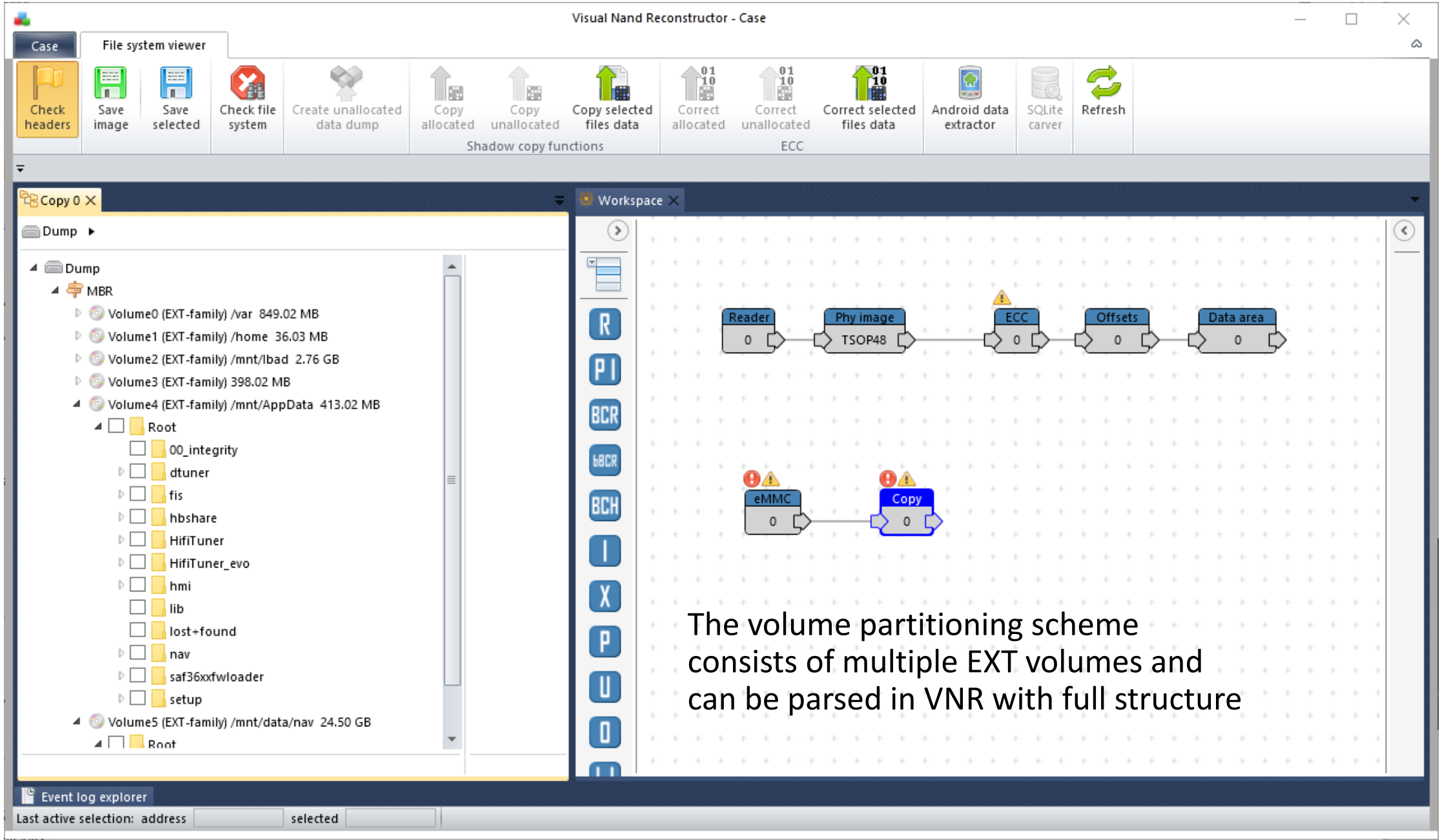


The eMMC memory chipBGA169/153 on the Main board

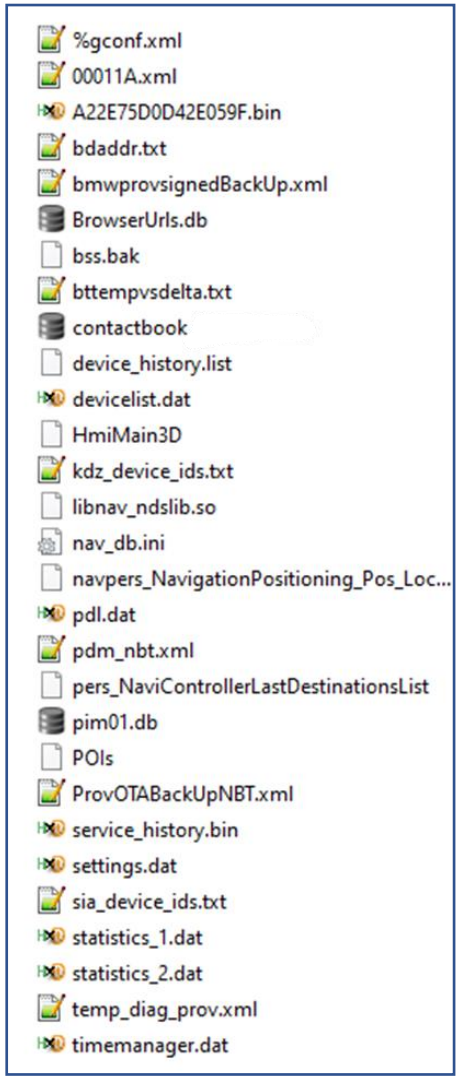
Classic eMMC memory can be read using one of adapters for Visual NAND Reconstructor



The memory is recognized in eMMC adapter and can be imaged



Plenty of files extracted from file system of eMMC



devicelist.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.ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000032   FF FF FF FF 02 00 00 00 5F 05 63 EB 43 43 3A 32  ÿÿÿÿ...._.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).ÿÿÿÿÿGala
00000160   78 79 20 41 37 20 28 32 30 31 38 29 00 FF FF FF  xy A7 (2018).ÿÿÿ
00000176   FF FF FF FF 0C 02 5A 00 07 00 00 00 1D 00 00 00  ÿÿÿÿ..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 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..ÿ
00000240   FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000256   FF FF FF FF 00 FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿ.ÿÿÿÿÿÿÿÿÿÿÿ
00000272   FF FF FF FF FF FF FF FF FF FF FF FF 00 00 00 00  ÿÿÿÿÿÿÿÿÿÿÿÿ....
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..ÿÿÿÿÿÿÿÿÿ
00000352   FF FF FF FF FF FF FF FF FF FF FF FF 00 FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿ.ÿÿÿ
00000368   FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000384   FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00  ÿÿÿÿ............
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..ÿ
00000448   FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000464   FF FF FF FF 00 FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿ.ÿÿÿÿÿÿÿÿÿÿÿ
00000480   FF FF FF FF FF FF FF FF FF FF FF FF 00 00 00 00  ÿÿÿÿÿÿÿÿÿÿÿÿ....
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

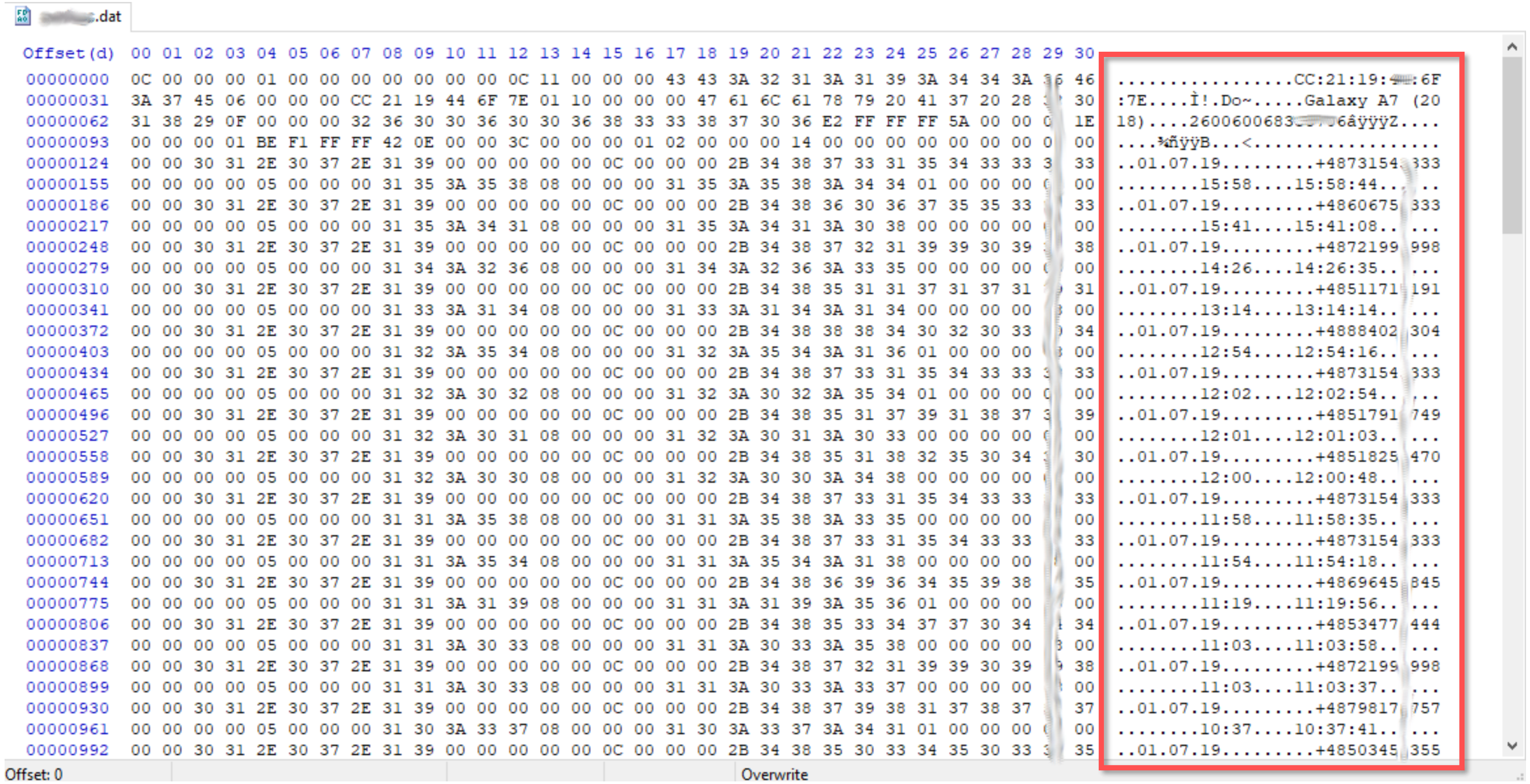
```
1
0
0
@END USB_STACK_INFO
##END DEVICE


##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

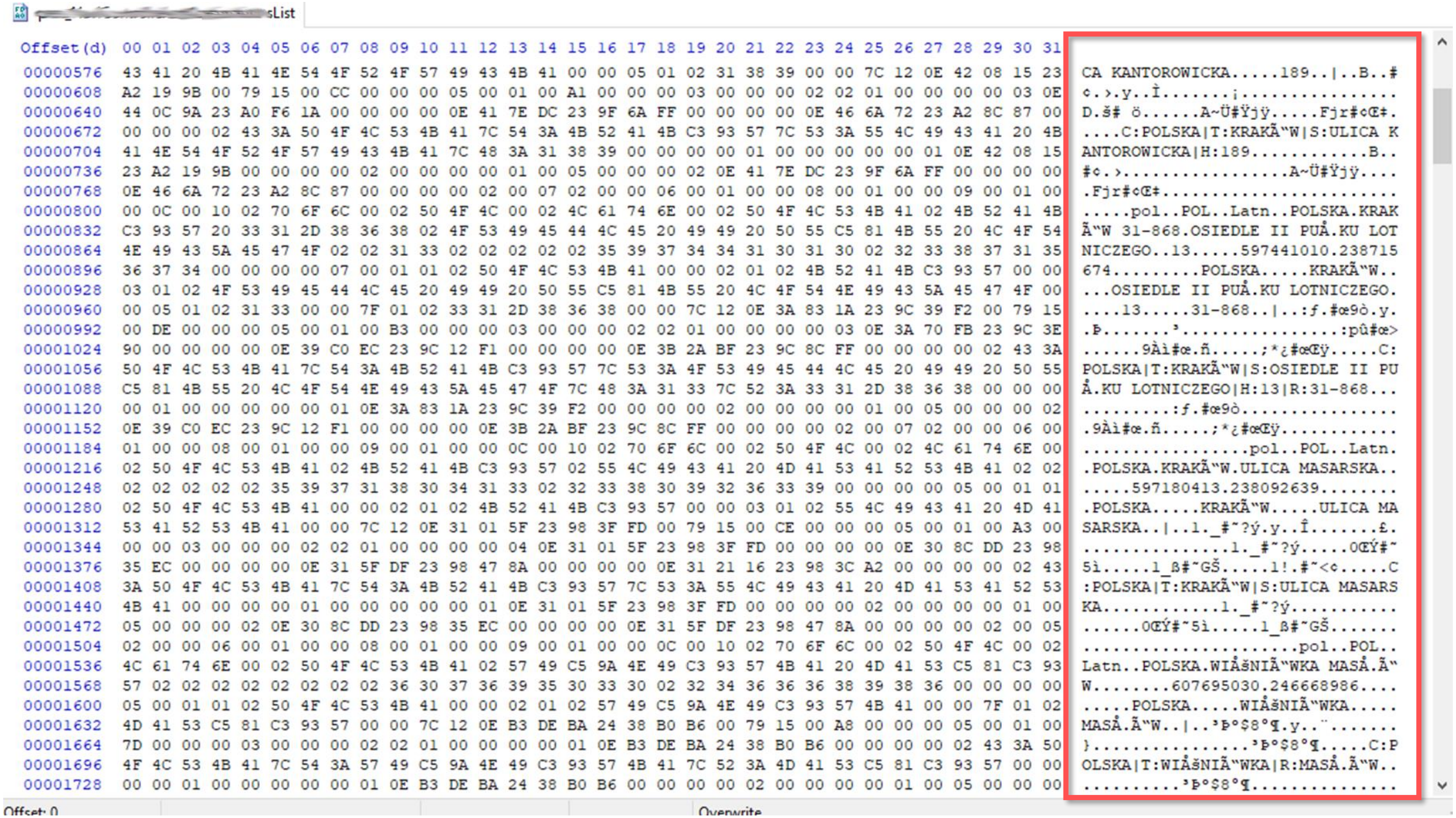
```
B82410181612
```

Device list of connected phones with their BT mac addresses

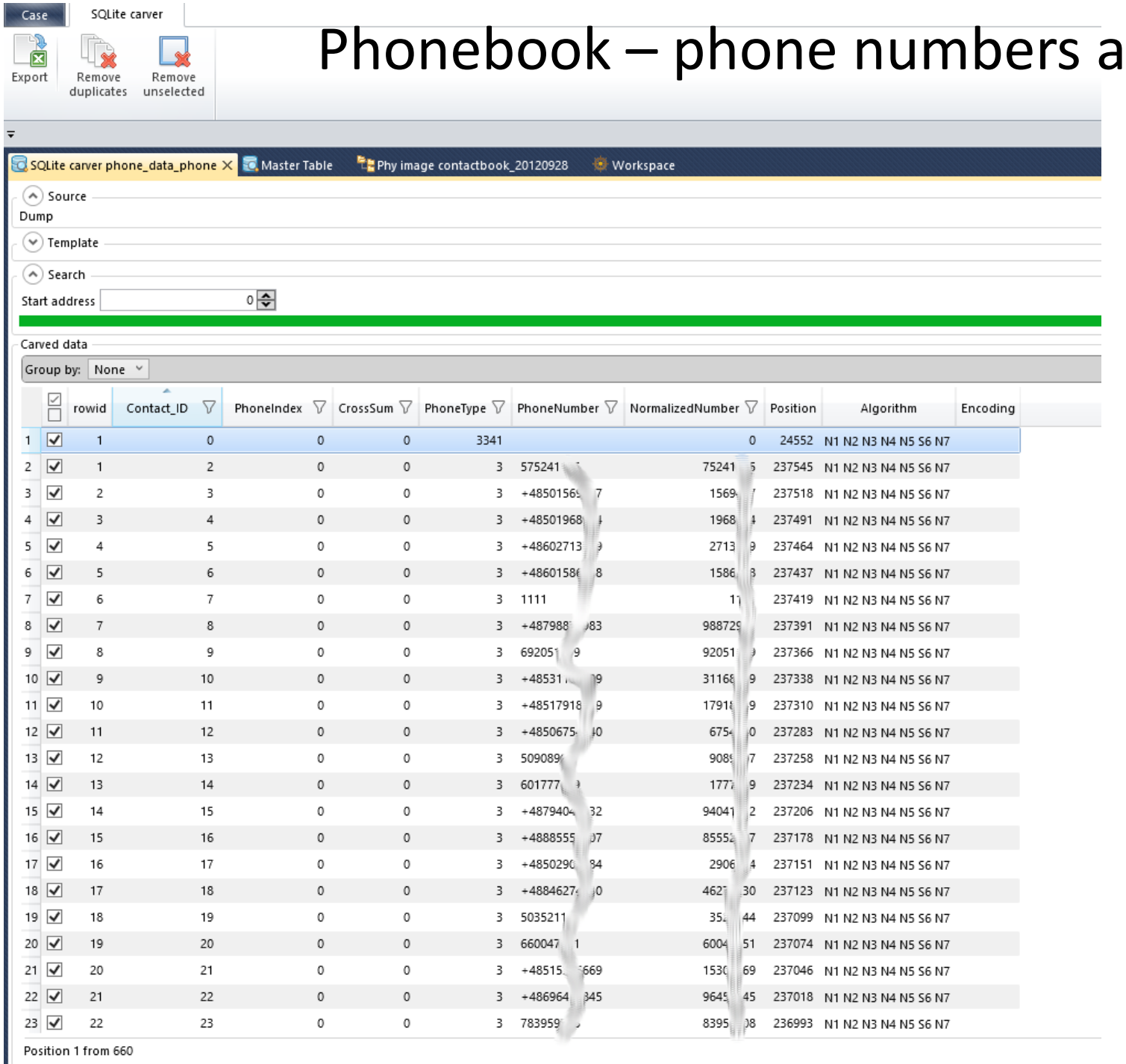
Call log history of connected phones with timestamps



Last destinations log



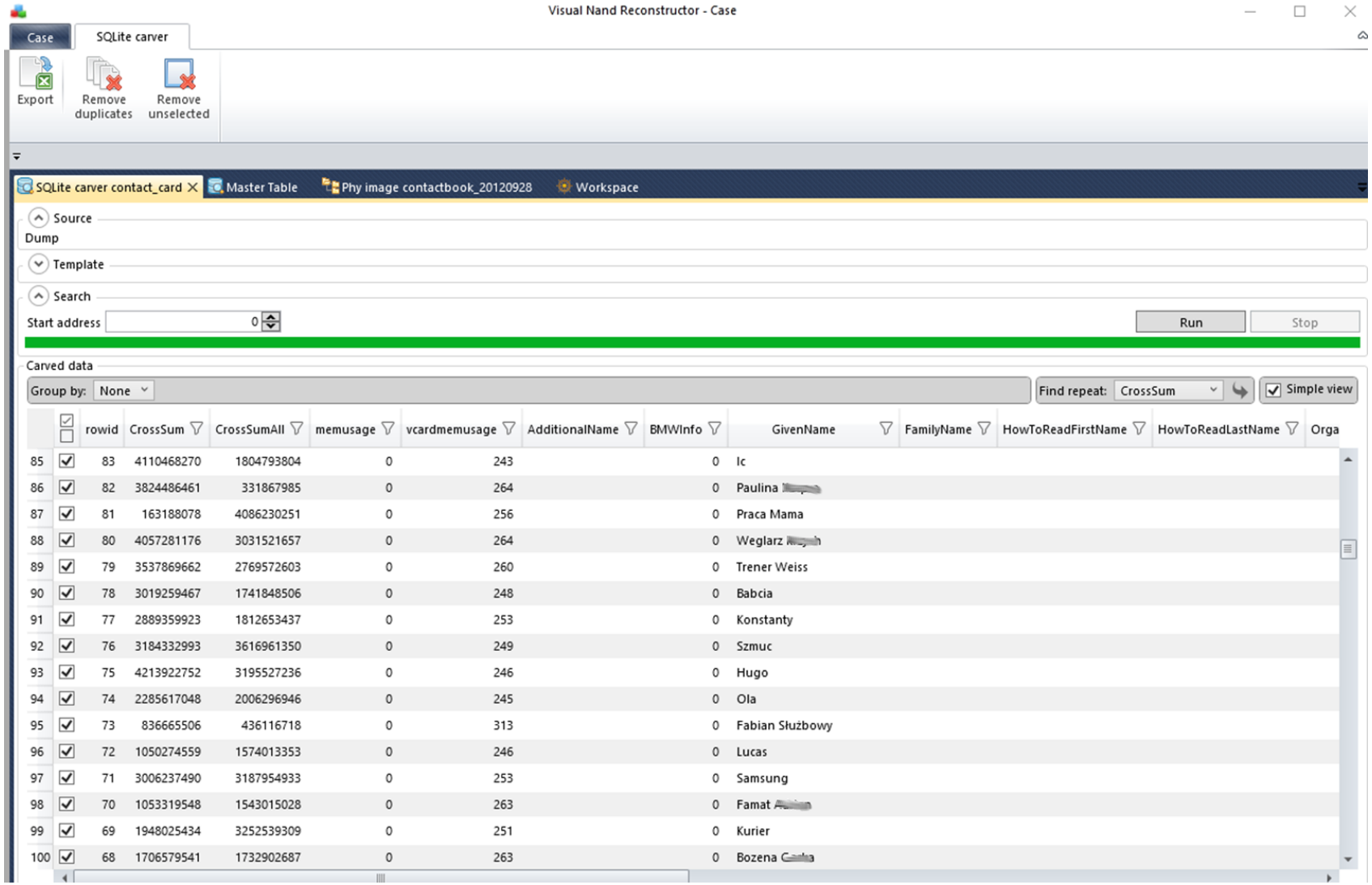
Phonebook – phone numbers and attributes



		rowid	Contact_ID	PhoneIndex	CrossSum	PhoneType	PhoneNumber	NormalizedNumber	Position	Algorithm	Encoding
1	☑	1	0	0	0	3341		0	24552	N1 N2 N3 N4 N5 S6 N7	
2	☑	1	2	0	0	3	575241	75241	237545	N1 N2 N3 N4 N5 S6 N7	
3	☑	2	3	0	0	3	+4850156 7	1569 7	237518	N1 N2 N3 N4 N5 S6 N7	
4	☑	3	4	0	0	3	+4850196 4	1968 4	237491	N1 N2 N3 N4 N5 S6 N7	
5	☑	4	5	0	0	3	+4860271 9	2713 9	237464	N1 N2 N3 N4 N5 S6 N7	
6	☑	5	6	0	0	3	+4860158 8	1586 8	237437	N1 N2 N3 N4 N5 S6 N7	
7	☑	6	7	0	0	3	1111	11	237419	N1 N2 N3 N4 N5 S6 N7	
8	☑	7	8	0	0	3	+487988 83	98872	237391	N1 N2 N3 N4 N5 S6 N7	
9	☑	8	9	0	0	3	692051 9	92051 9	237366	N1 N2 N3 N4 N5 S6 N7	
10	☑	9	10	0	0	3	+48531 9	31168 9	237338	N1 N2 N3 N4 N5 S6 N7	
11	☑	10	11	0	0	3	+485179 9	1791 9	237310	N1 N2 N3 N4 N5 S6 N7	
12	☑	11	12	0	0	3	+485067 0	675 0	237283	N1 N2 N3 N4 N5 S6 N7	
13	☑	12	13	0	0	3	509089	908 7	237258	N1 N2 N3 N4 N5 S6 N7	
14	☑	13	14	0	0	3	601777	177 9	237234	N1 N2 N3 N4 N5 S6 N7	
15	☑	14	15	0	0	3	+487940 32	94041 2	237206	N1 N2 N3 N4 N5 S6 N7	
16	☑	15	16	0	0	3	+488855 07	8555 7	237178	N1 N2 N3 N4 N5 S6 N7	
17	☑	16	17	0	0	3	+485029 84	2906 4	237151	N1 N2 N3 N4 N5 S6 N7	
18	☑	17	18	0	0	3	+488462 0	462 30	237123	N1 N2 N3 N4 N5 S6 N7	
19	☑	18	19	0	0	3	5035211	35 44	237099	N1 N2 N3 N4 N5 S6 N7	
20	☑	19	20	0	0	3	660047 1	600 51	237074	N1 N2 N3 N4 N5 S6 N7	
21	☑	20	21	0	0	3	+48515 669	153 69	237046	N1 N2 N3 N4 N5 S6 N7	
22	☑	21	22	0	0	3	+486964 345	964 45	237018	N1 N2 N3 N4 N5 S6 N7	
23	☑	22	23	0	0	3	783959	839 08	236993	N1 N2 N3 N4 N5 S6 N7	

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



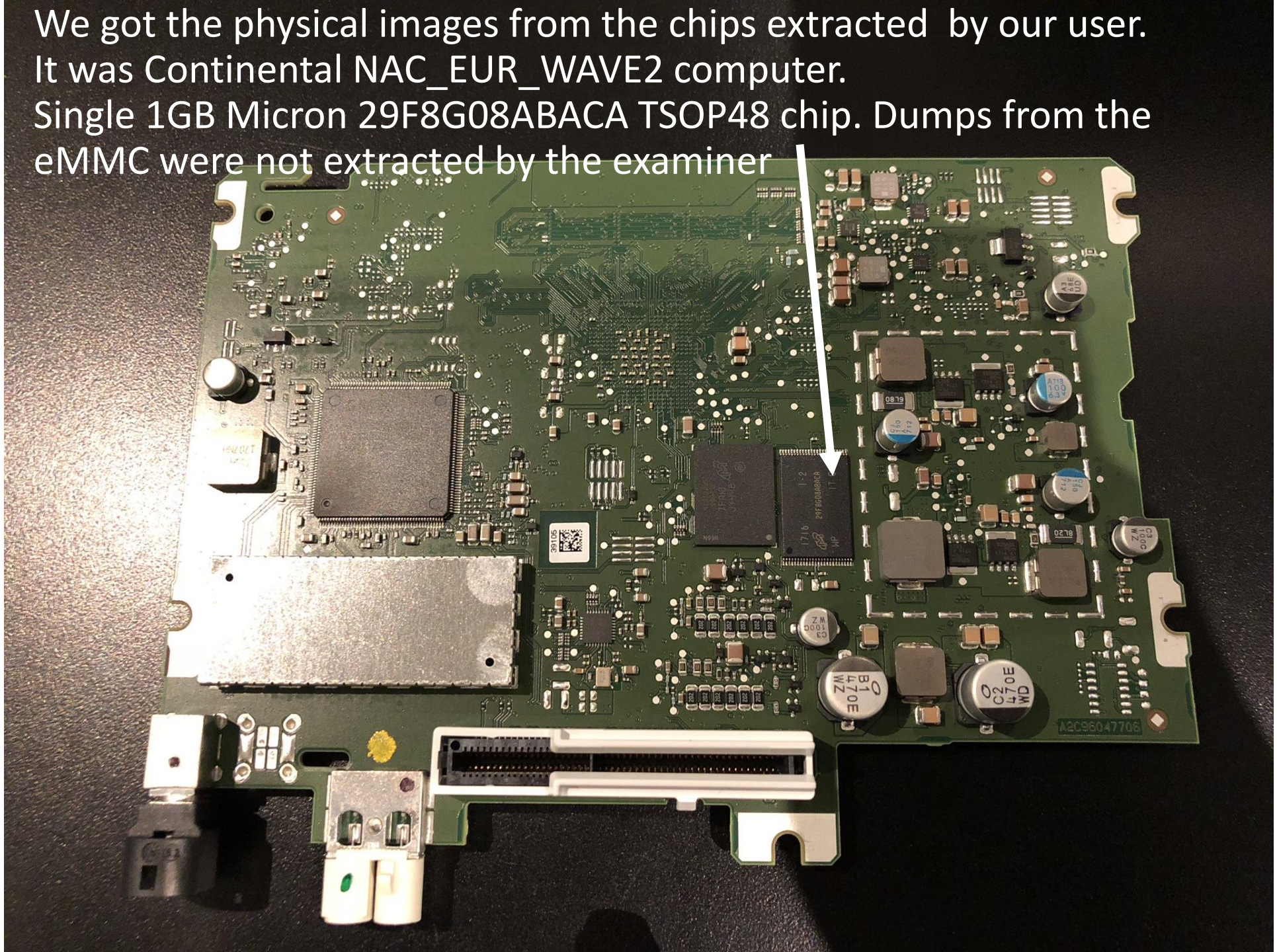
		rowid	CrossSum	CrossSumAll	memusage	vcardmemusage	AdditionalName	BMWInfo	GivenName	FamilyName	HowToReadFirstName	HowToReadLastName	Orga
85	☑	83	4110468270	1804793804	0	243		0	Ic				
86	☑	82	3824486461	331867985	0	264		0	Paulina				
87	☑	81	163188078	4086230251	0	256		0	Praca Mama				
88	☑	80	4057281176	3031521657	0	264		0	Weglarz				
89	☑	79	3537869662	2769572603	0	260		0	Trener Weiss				
90	☑	78	3019259467	1741848506	0	248		0	Babcia				
91	☑	77	2889359923	1812653437	0	253		0	Konstanty				
92	☑	76	3184332993	3616961350	0	249		0	Szmuc				
93	☑	75	4213922752	3195527236	0	246		0	Hugo				
94	☑	74	2285617048	2006296946	0	245		0	Ola				
95	☑	73	836665506	436116718	0	313		0	Fabian Służbowy				
96	☑	72	1050274559	1574013353	0	246		0	Lucas				
97	☑	71	3006237490	3187954933	0	253		0	Samsung				
98	☑	70	1053319548	1543015028	0	263		0	Famat				
99	☑	69	1948025434	3252539309	0	251		0	Kurier				
100	☑	68	1706579541	1732902687	0	263		0	Bozena				

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

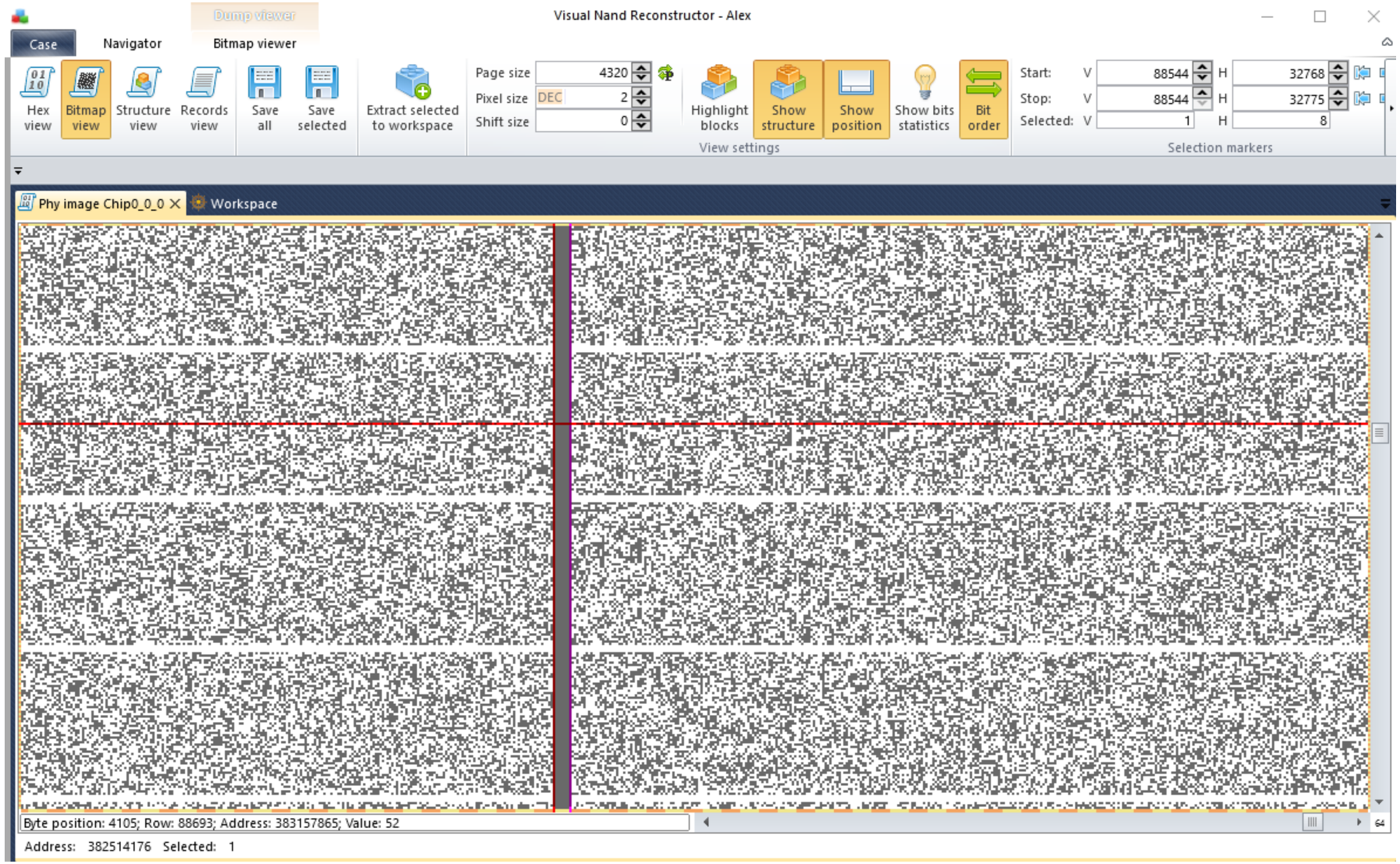
This kind of evidence is priceless when attempting to establish the forensic facts.

https://bi.im-g.pl/im/c8/9e/15/z22668488IH,Citroen-C3-Aircross.jpg

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

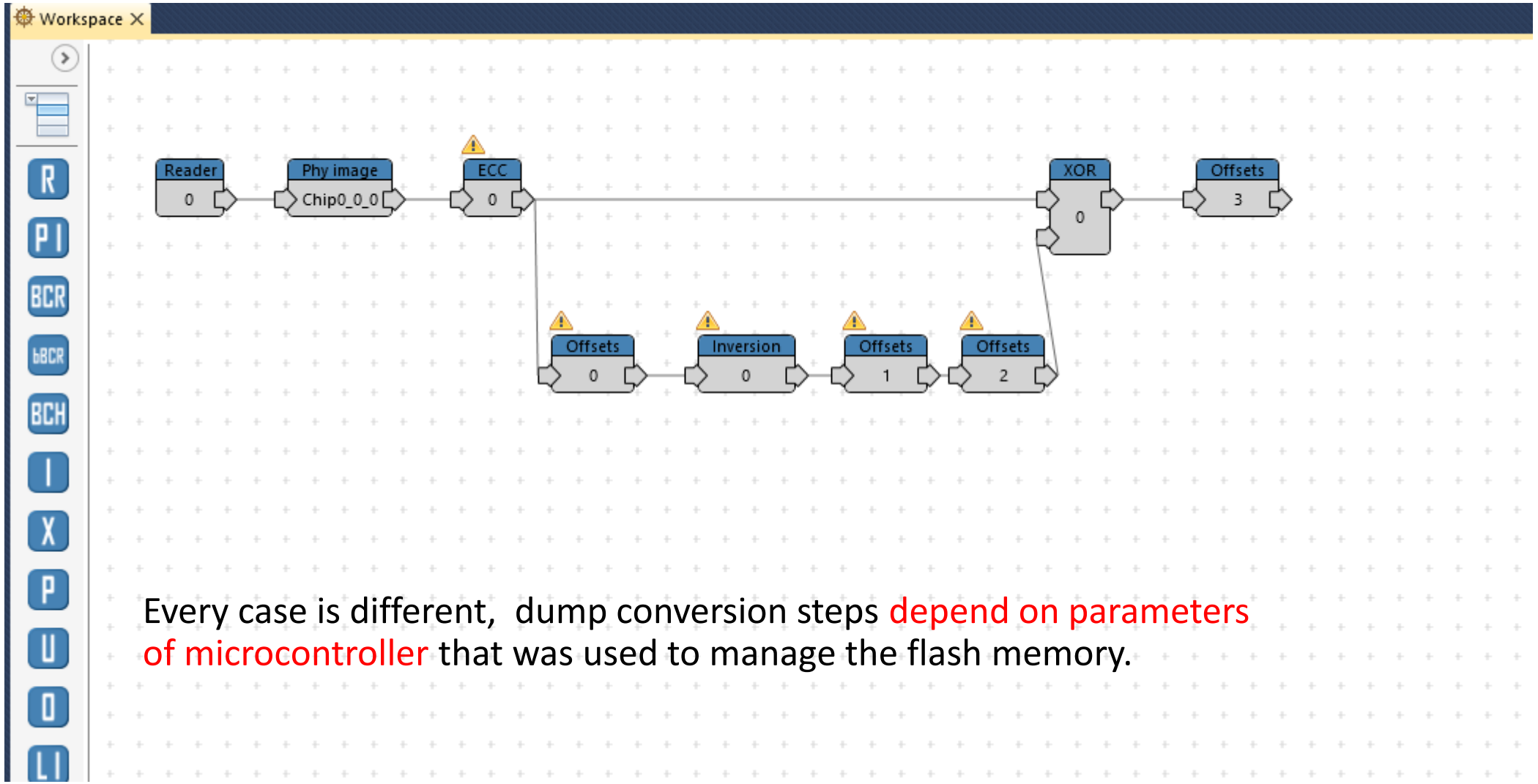


The memory dump through the bitmap



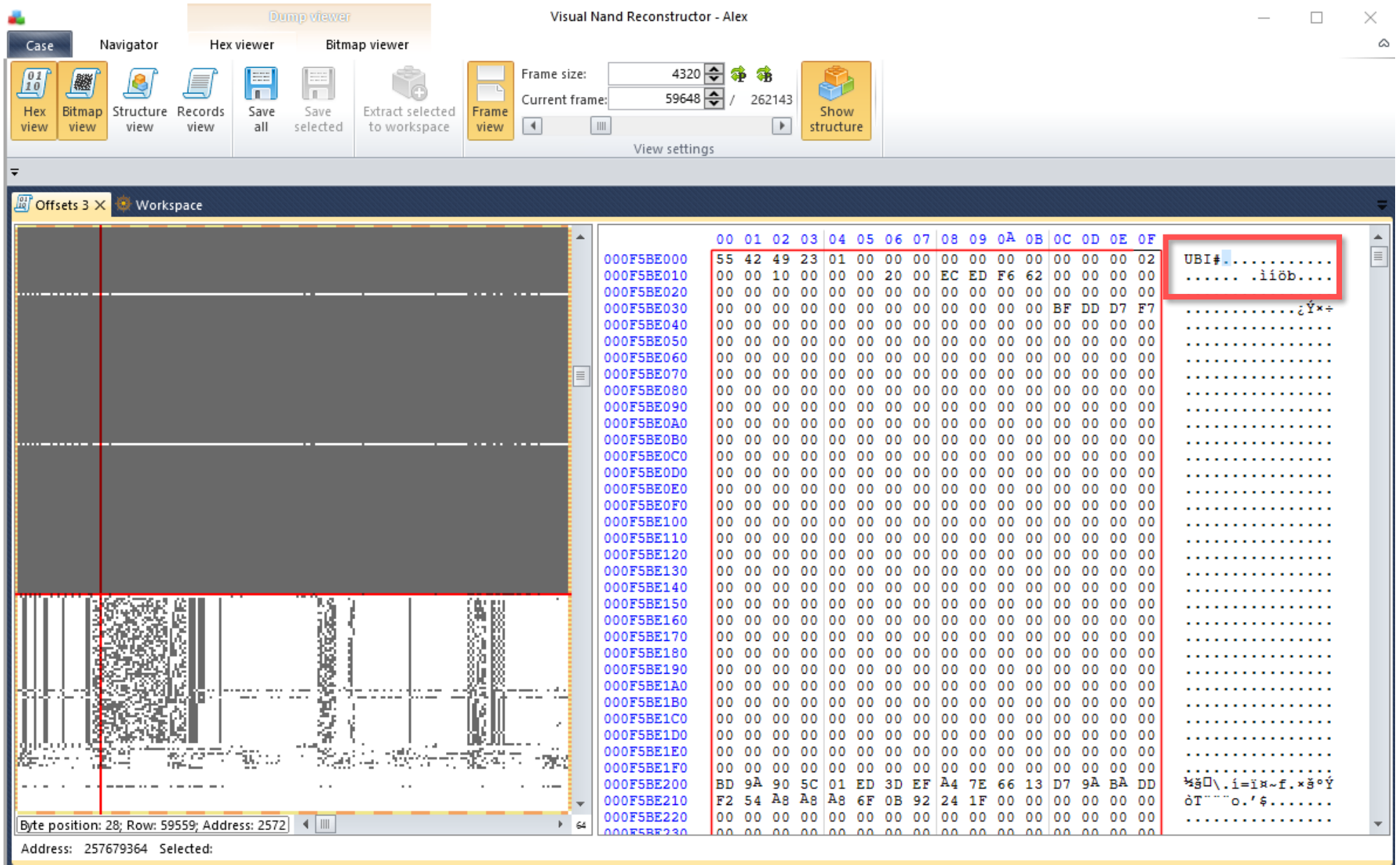
The bitmap helps to analyze and separate spare area of memory from the actual user's data area.

Emulation of controller’s conversion workflow



Every case is different, dump conversion steps depend on parameters of microcontroller that was used to manage the flash memory.

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



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 | New Record | Delete Record

	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

|< < 1 - 13 of 20 > >| Go to: 1

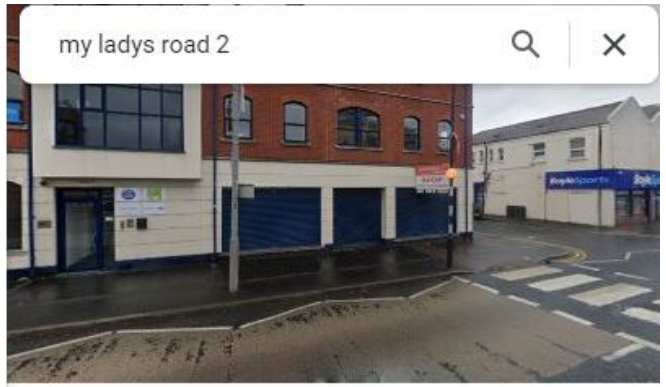
Mode: Binary | Import | Export | Set as NULL

```
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.m.....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
```

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

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

Apply



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 miejsce

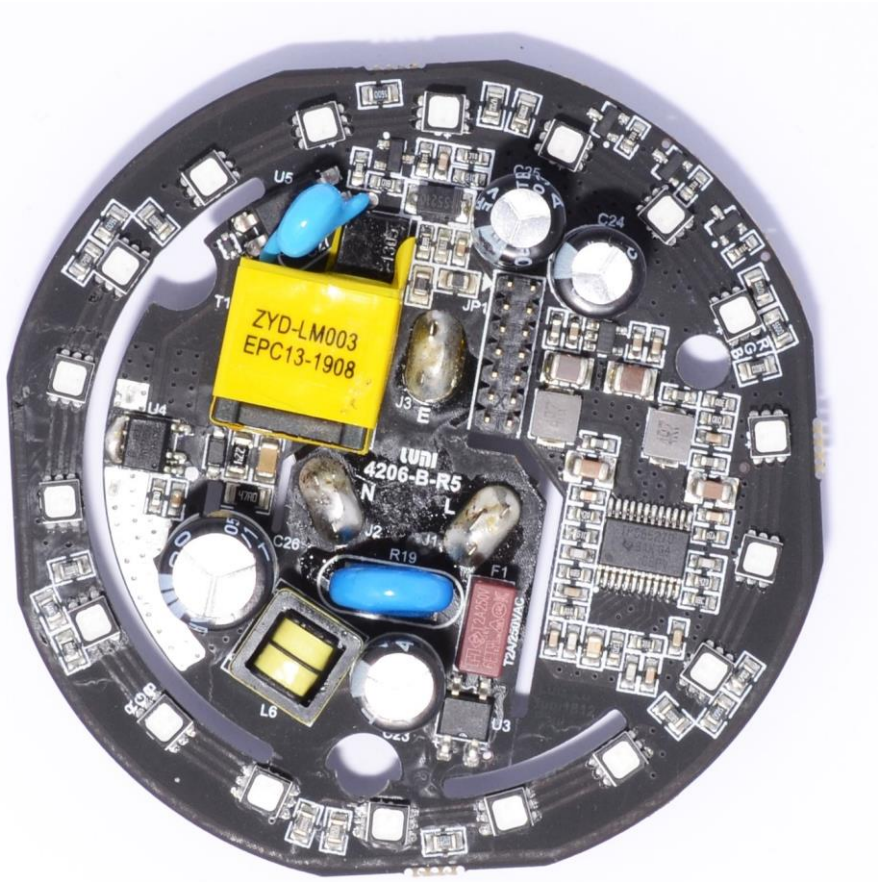
Dodaj swoją firmę

Dodaj etykietę

Xiaomi smart home gateway/hub V2 DGNWG05LM

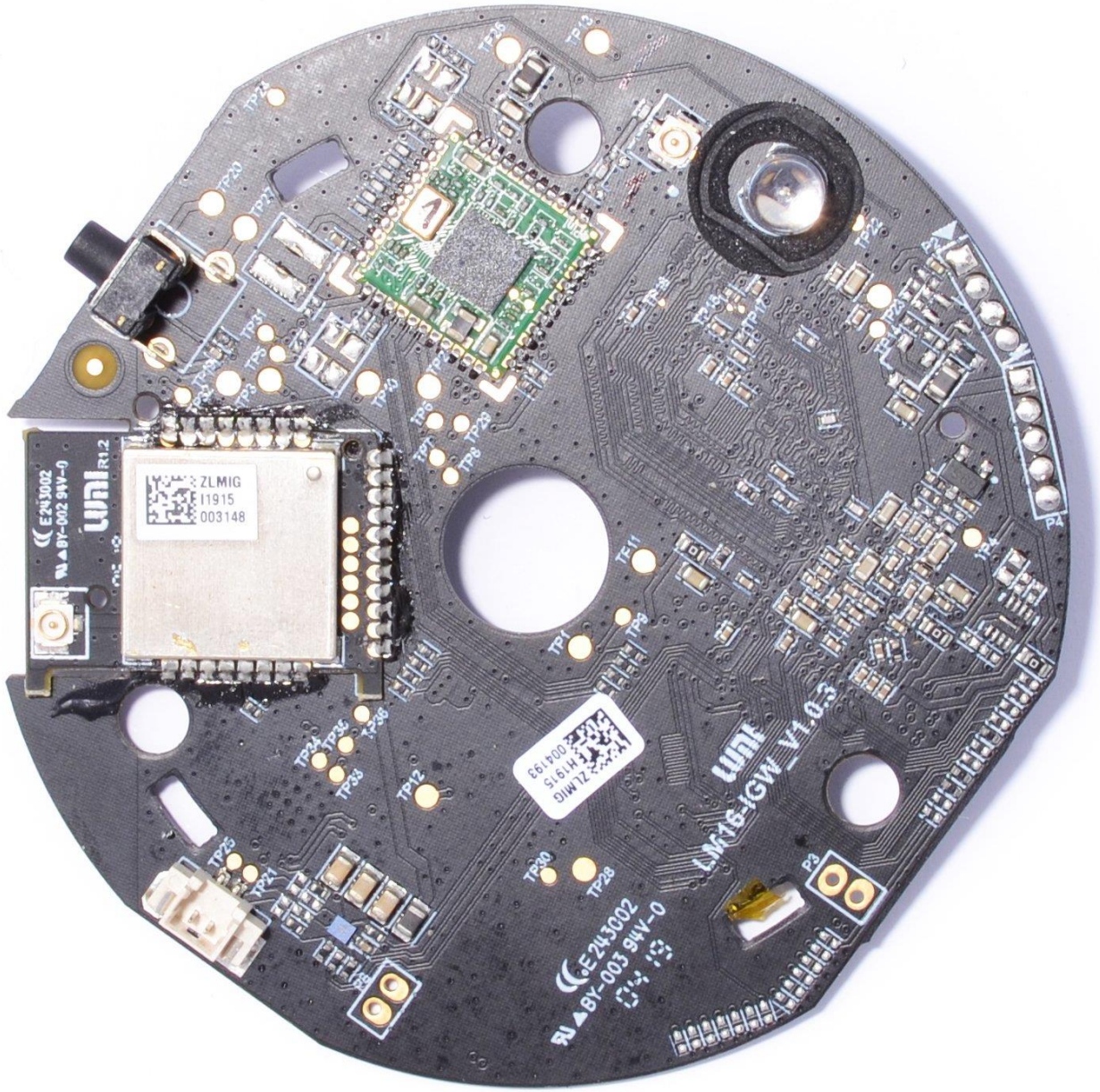
The device is used as a Wi-Fi, ZigBee and Bluetooth hub for the smart home sensors and automations (e.g. motion sensor, door lock sensor, water sensor, cameras, etc)

Analog PCB both sides



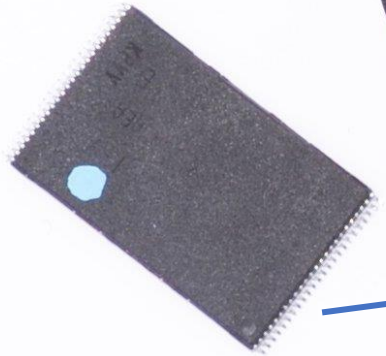
The hub consists of two PCBs connected together. Analog PCB has nothing interesting since it’s only power-related. Its functions are to convert AC from the wall socket to the digital board, power management, pwm led controller, leds, etc)

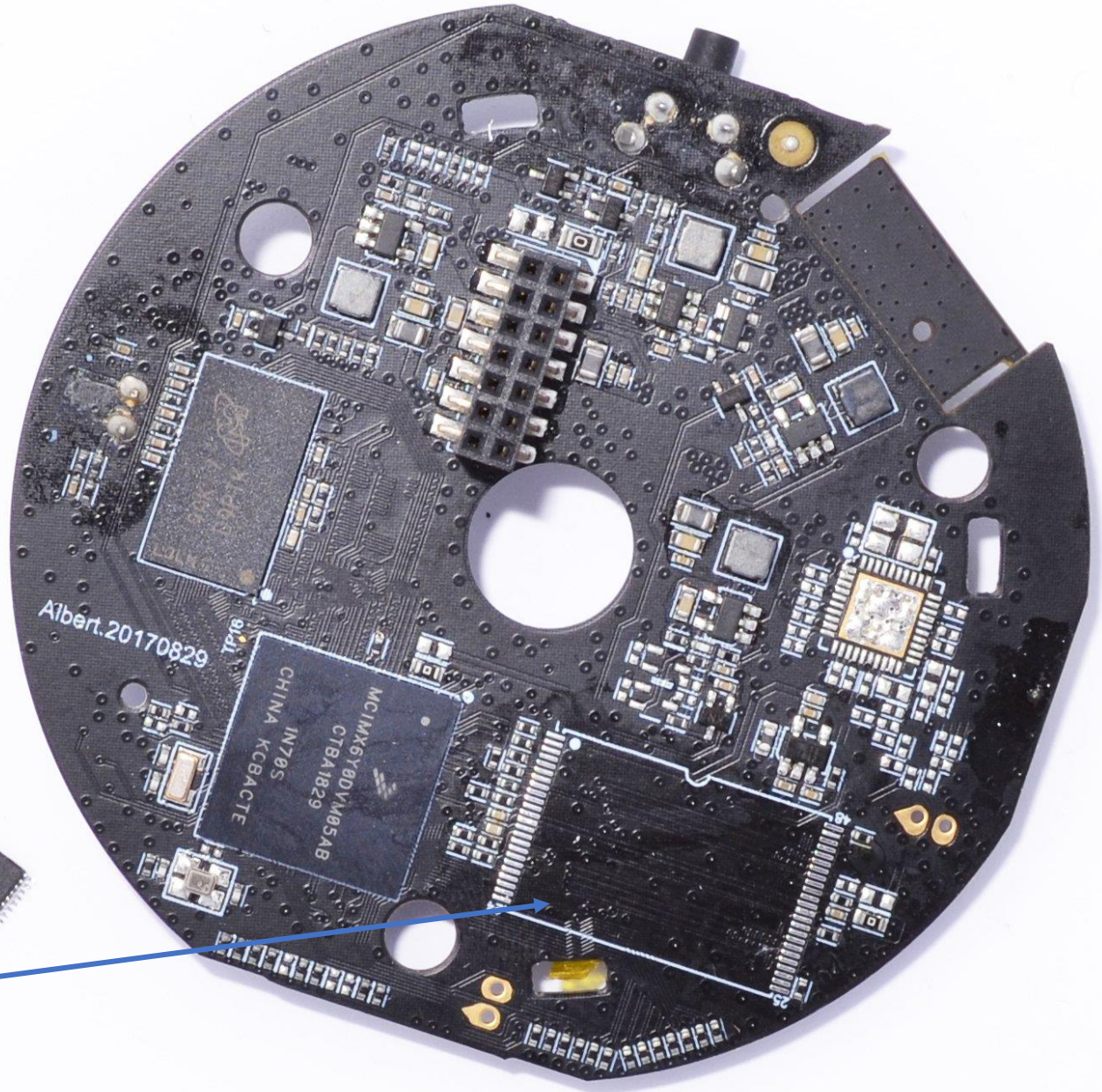
Digital PCB top side (ZigBee, Wi-FI modules)



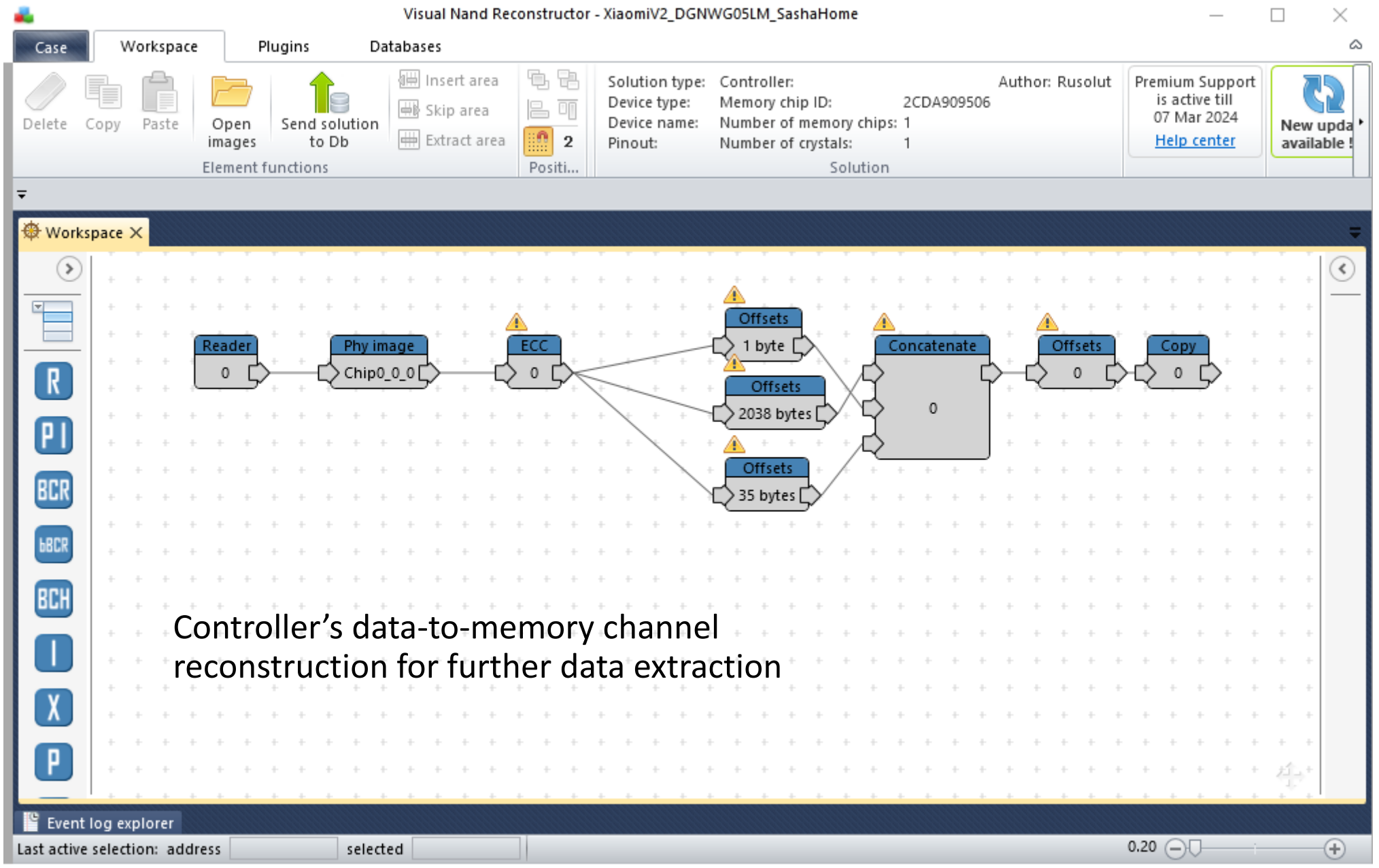
Digital PCB bottom side (MCU, NAND, RAM)

TSOP48 NAND

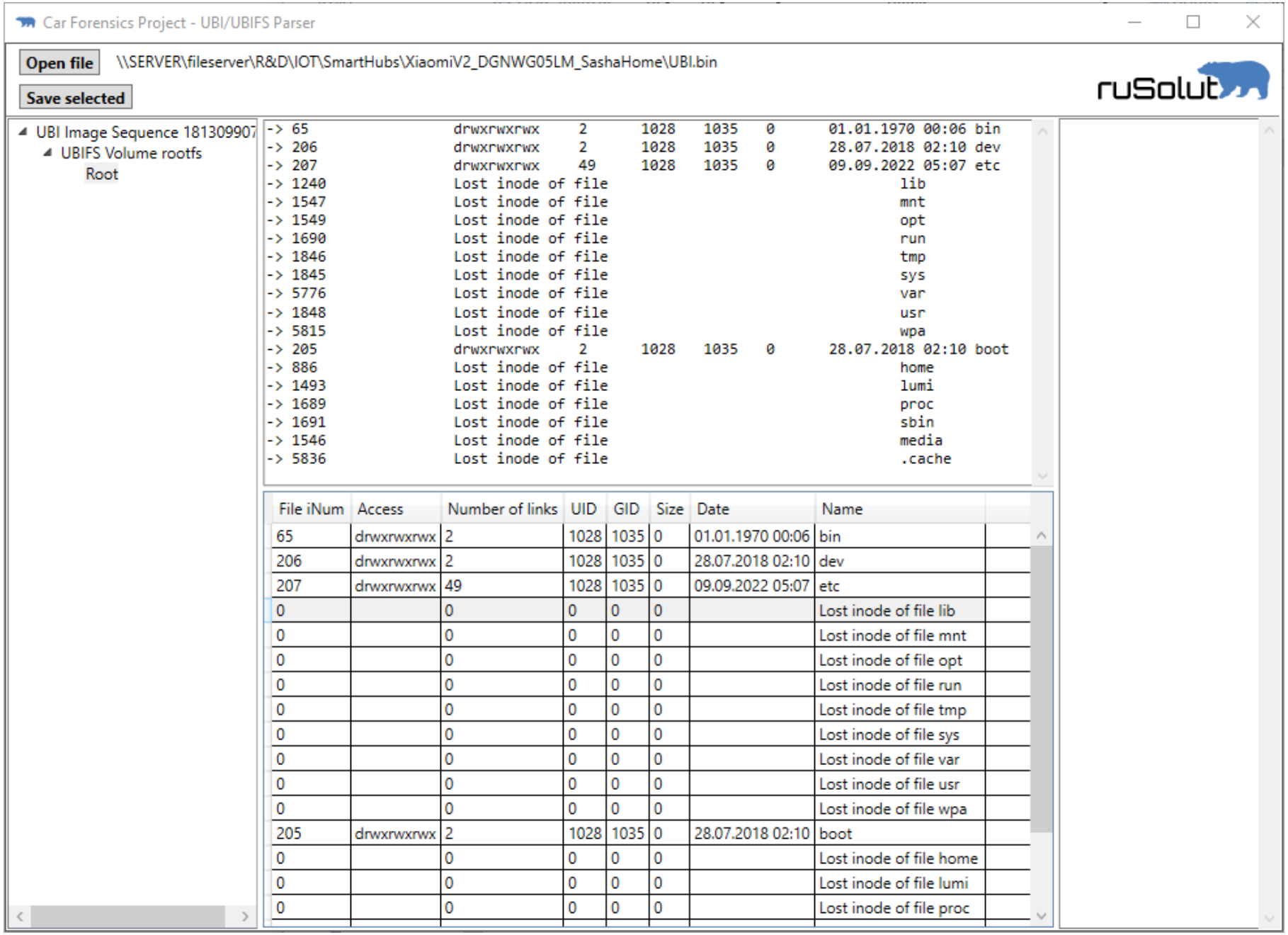




The NAND memory was read via VNR reader

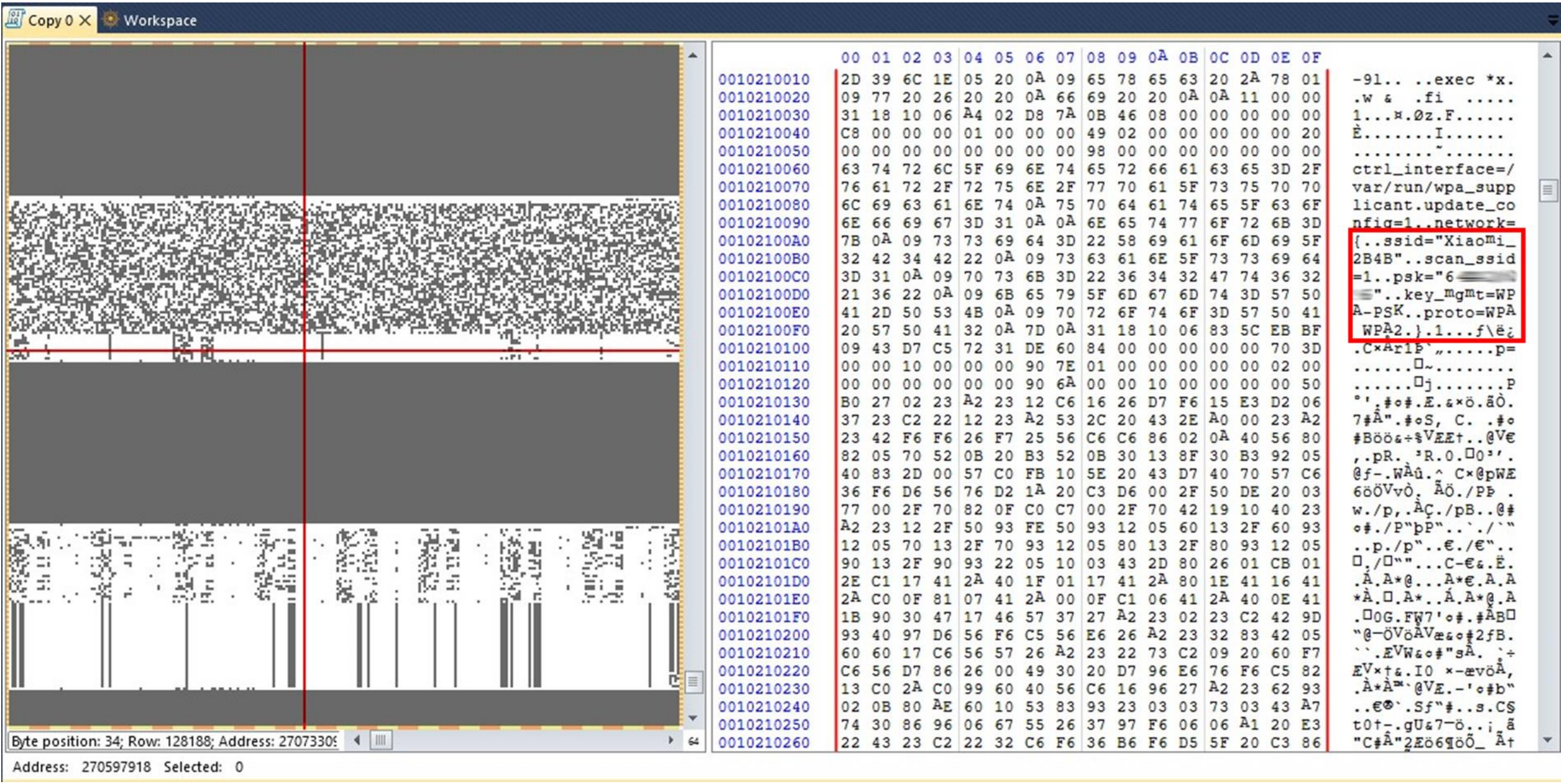


UBIFS file system volume (device was possibly reset, since many lost iNodes)



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



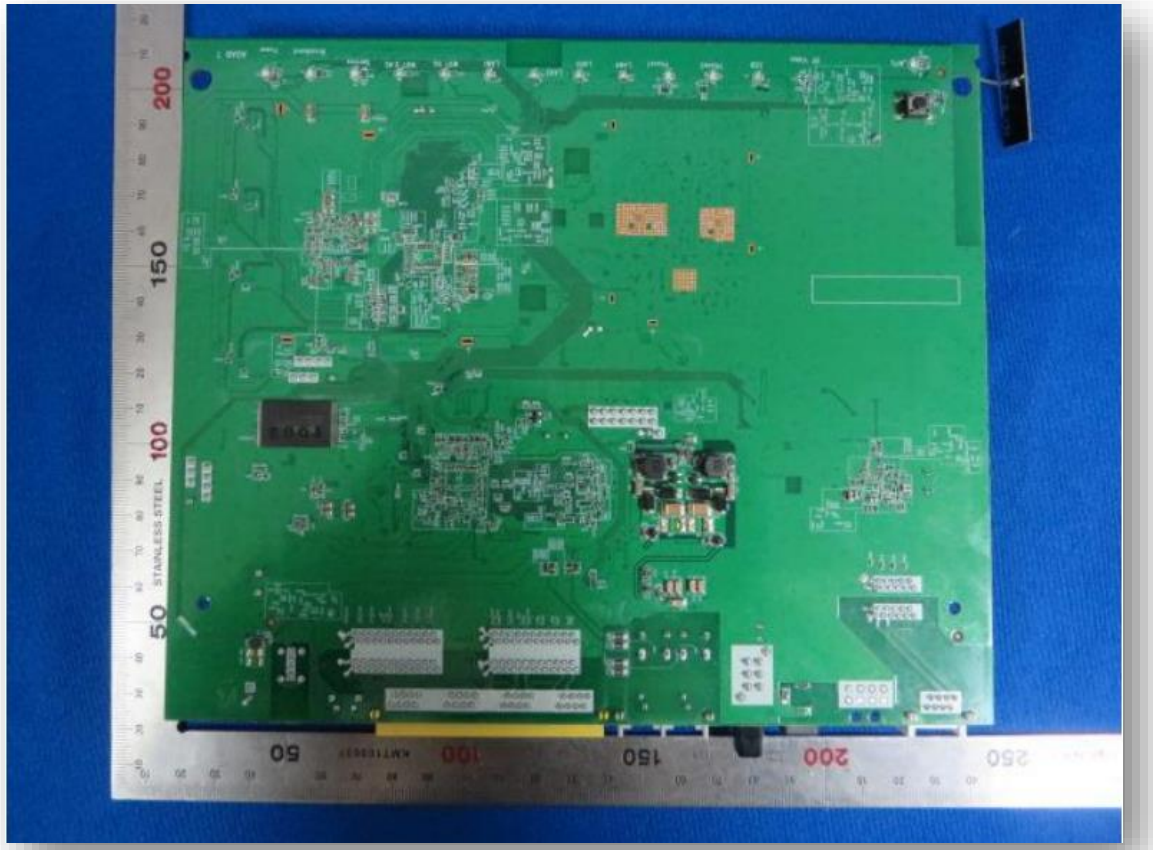
Router CALIX 844E-1

https://telecomcauliffe.com/wp-content/uploads/2021/05/TELECOMCAULIFFE_PICS-TELECOM_For-Sale-Calix-813G-1-GigaCenters-100-04800_05.21.png

Admin panel

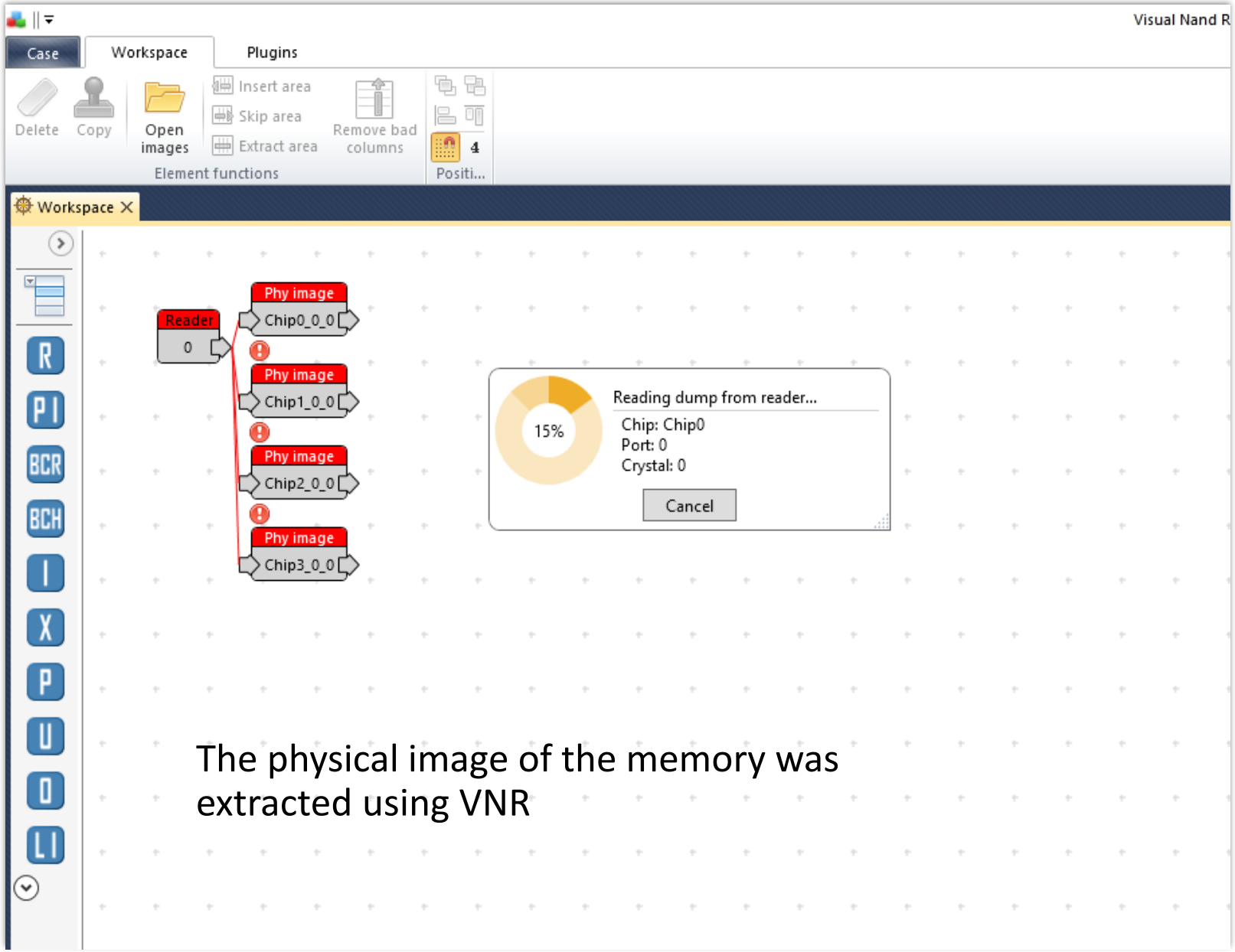
In this case forensic expert had no login credentials for the seized device

Electronic board and memory chip (TSOP48)



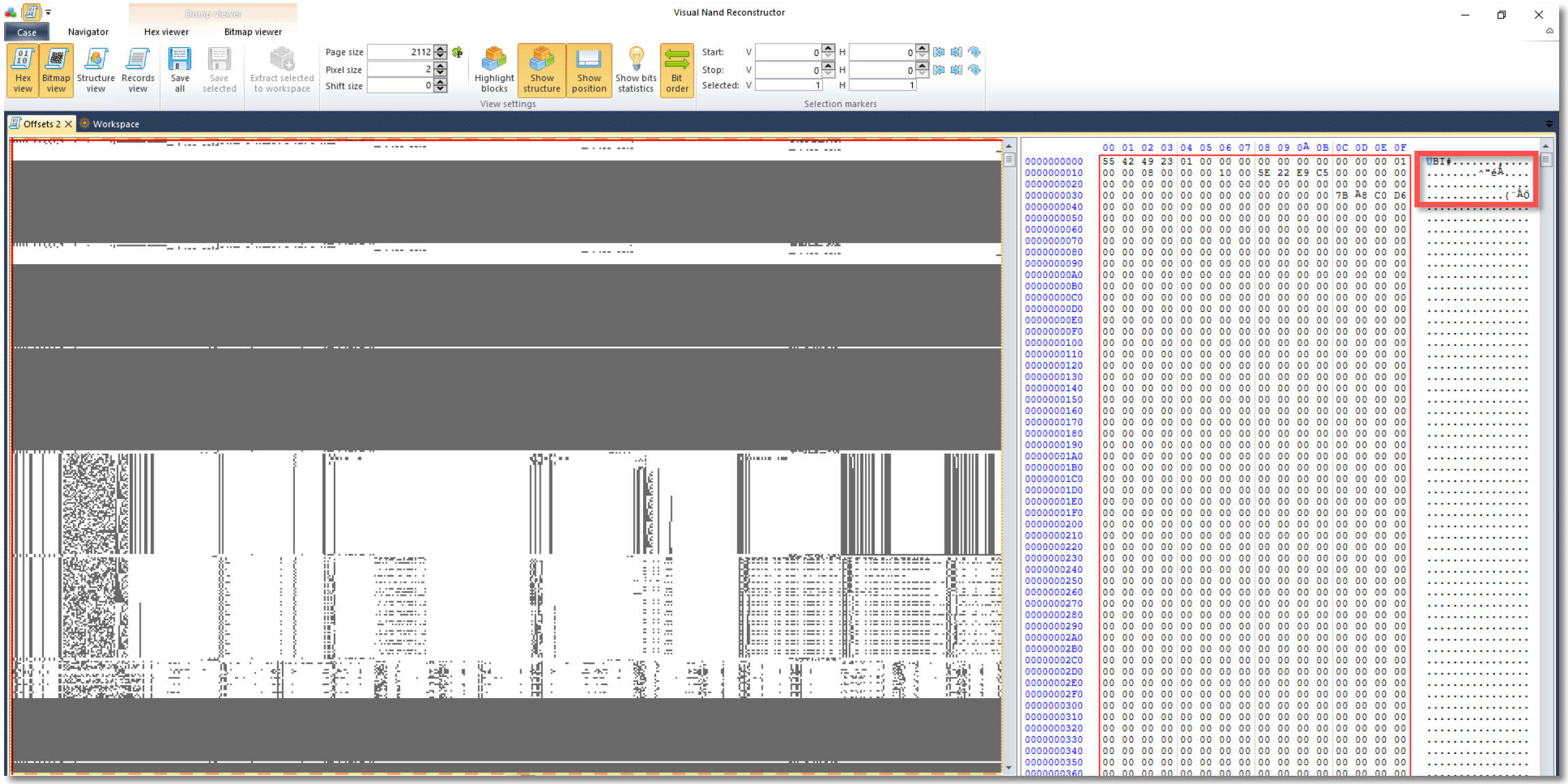
The device was disassembled to get access to the data in the memory chip

NAND memory reading

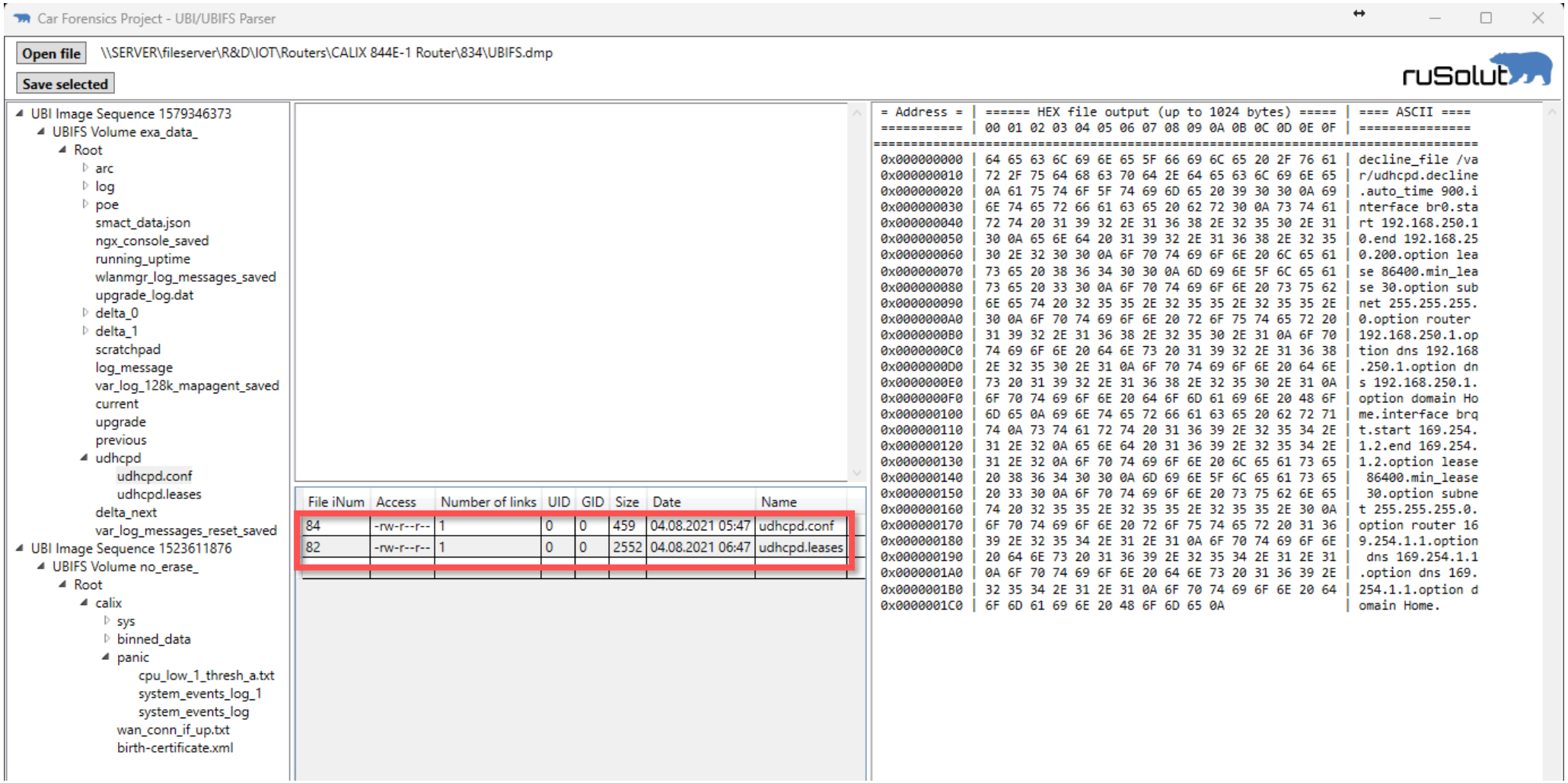


The physical image of the memory was extracted using VNR

UBIFS was detected (a very popular file system in embedded devices)

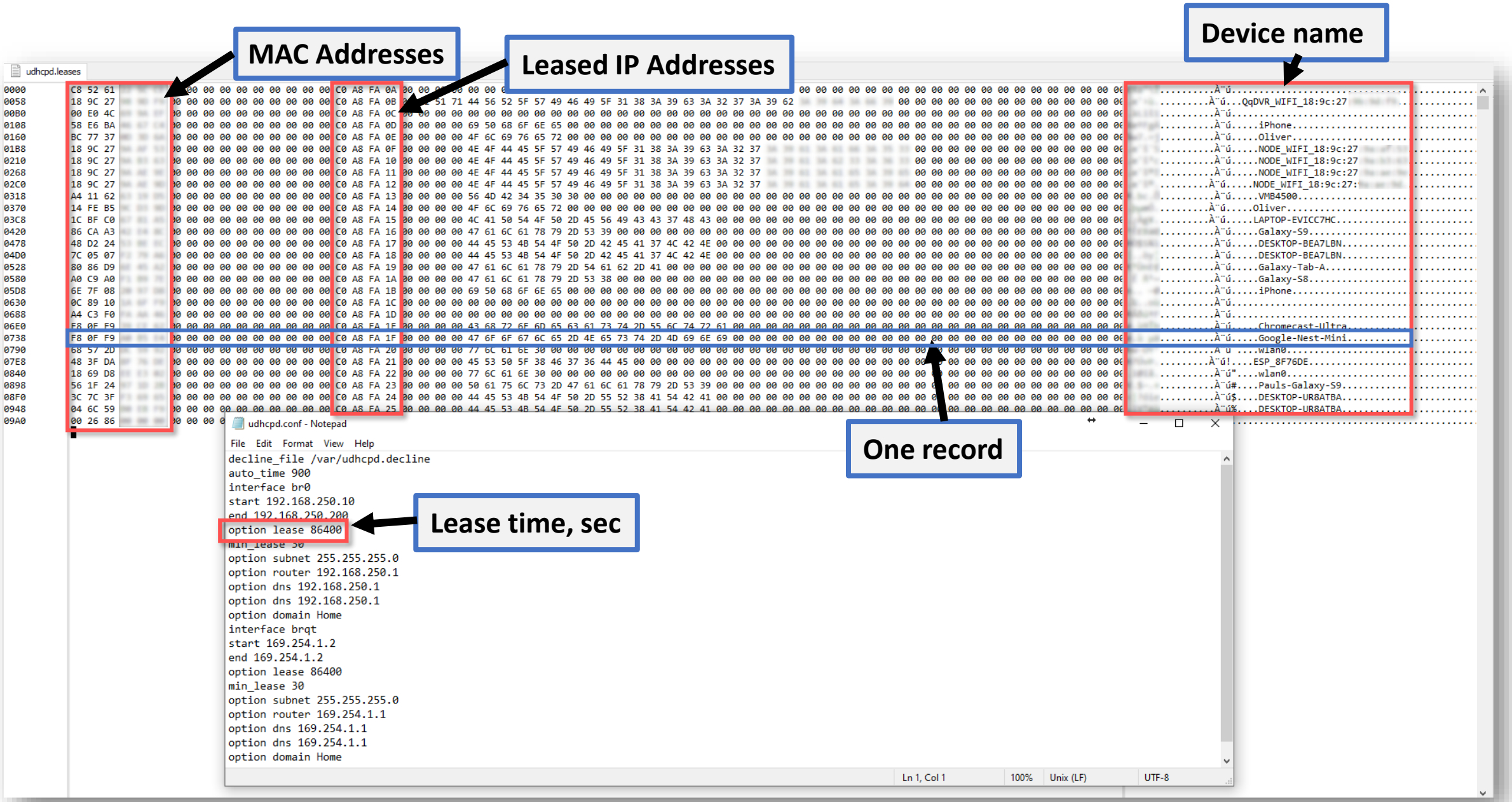


The file system reconstruction



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.

DHCP leases log

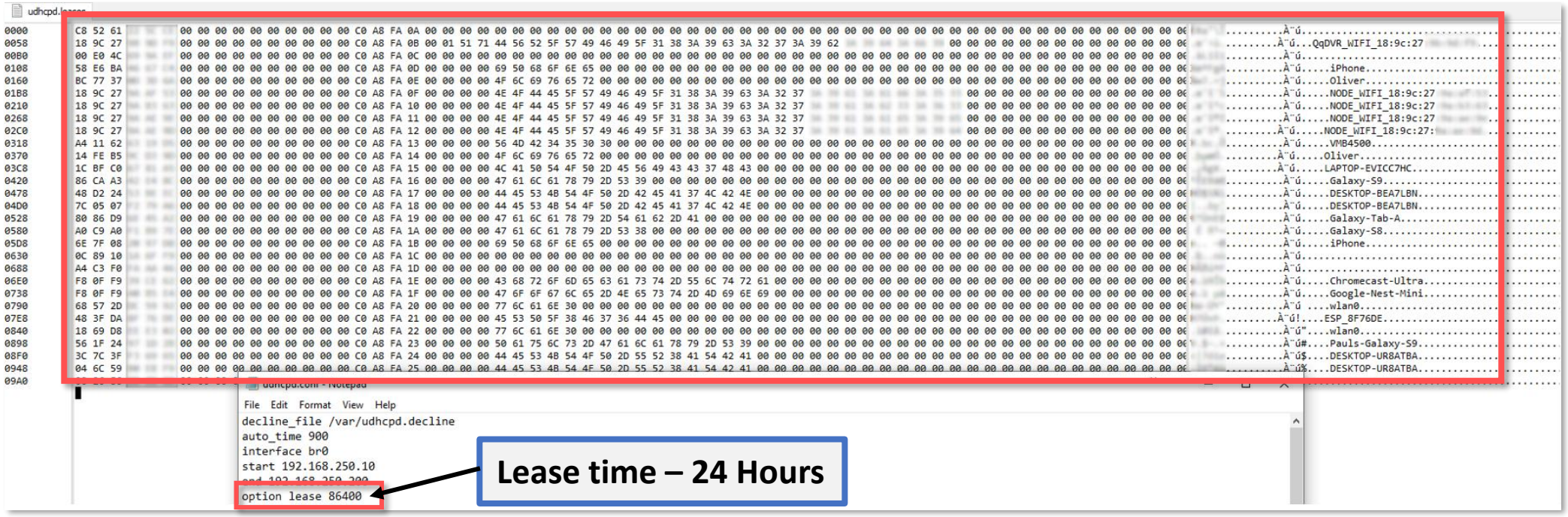


IP address rent-time is 24 hours, so all devices mentioned in the UDHCPD.leases file were connected to the network within 24 hours, starting from file creation date

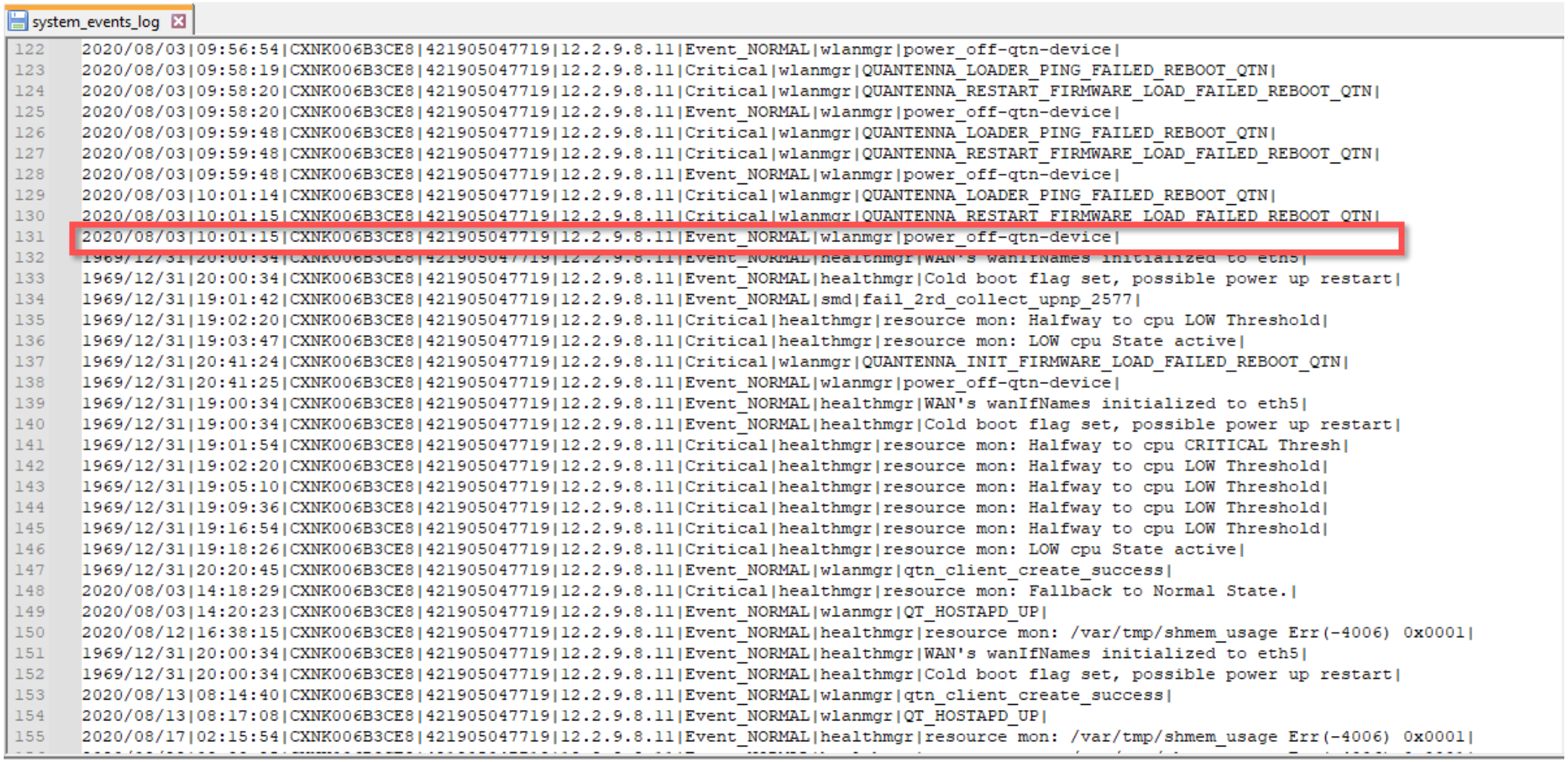
udhcpd.leases
delta_next
var_log_messages_reset_saved
UBI Image Sequence 1523611876
UBIFS Volume no_erase_
Root

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

04/08/2021 06:47
File creation date



Lease time – 24 Hours



system_events_log

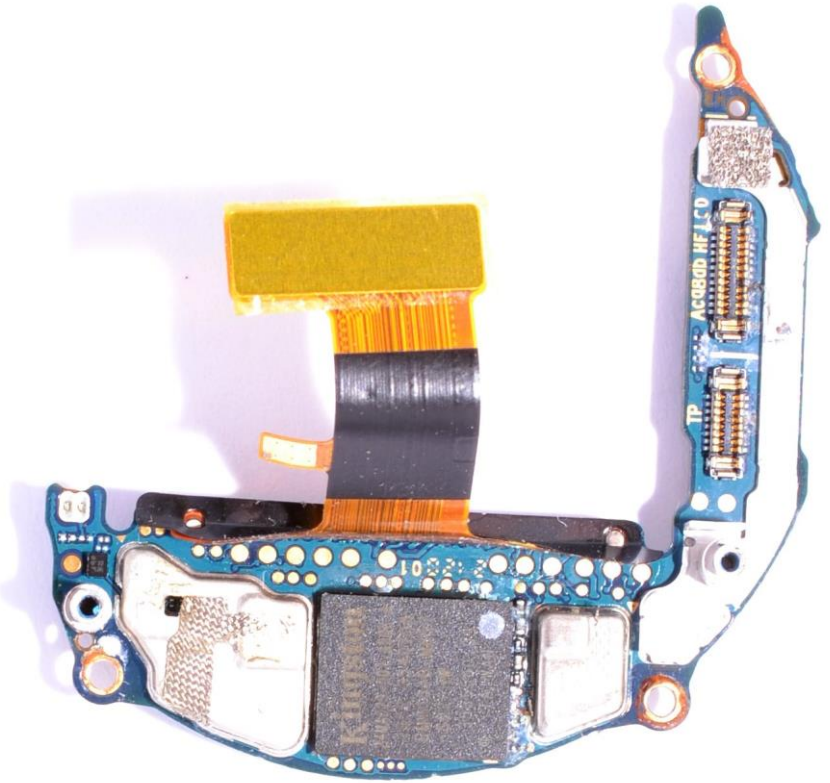
```
2020/08/03|09:56:54|CXNK006B3CE8|421905047719|12.2.9.8.11|Event_NORMAL|wlanmgr|power_off-qtn-device|
2020/08/03|09:58:19|CXNK006B3CE8|421905047719|12.2.9.8.11|Critical|wlanmgr|QUANTENNA_LOADER_PING_FAILED_REBOOT_QTN|
2020/08/03|09:58:20|CXNK006B3CE8|421905047719|12.2.9.8.11|Critical|wlanmgr|QUANTENNA_RESTART_FIRMWARE_LOAD_FAILED_REBOOT_QTN|
2020/08/03|09:58:20|CXNK006B3CE8|421905047719|12.2.9.8.11|Event_NORMAL|wlanmgr|power_off-qtn-device|
2020/08/03|09:59:48|CXNK006B3CE8|421905047719|12.2.9.8.11|Critical|wlanmgr|QUANTENNA_LOADER_PING_FAILED_REBOOT_QTN|
2020/08/03|09:59:48|CXNK006B3CE8|421905047719|12.2.9.8.11|Critical|wlanmgr|QUANTENNA_RESTART_FIRMWARE_LOAD_FAILED_REBOOT_QTN|
2020/08/03|09:59:48|CXNK006B3CE8|421905047719|12.2.9.8.11|Event_NORMAL|wlanmgr|power_off-qtn-device|
2020/08/03|10:01:14|CXNK006B3CE8|421905047719|12.2.9.8.11|Critical|wlanmgr|QUANTENNA_LOADER_PING_FAILED_REBOOT_QTN|
2020/08/03|10:01:15|CXNK006B3CE8|421905047719|12.2.9.8.11|Critical|wlanmgr|QUANTENNA_RESTART_FIRMWARE_LOAD_FAILED_REBOOT_QTN|
2020/08/03|10:01:15|CXNK006B3CE8|421905047719|12.2.9.8.11|Event_NORMAL|wlanmgr|power_off-qtn-device|
1969/12/31|20:00:34|CXNK006B3CE8|421905047719|12.2.9.8.11|Event_NORMAL|healthmgr|WAN's wanIfNames initialized to eth5|
1969/12/31|20:00:34|CXNK006B3CE8|421905047719|12.2.9.8.11|Event_NORMAL|healthmgr|Cold boot flag set, possible power up restart|
1969/12/31|19:01:42|CXNK006B3CE8|421905047719|12.2.9.8.11|Event_NORMAL|smd|fail_2rd_collect_upnp_2577|
1969/12/31|19:02:20|CXNK006B3CE8|421905047719|12.2.9.8.11|Critical|healthmgr|resource mon: Halfway to cpu LOW Threshold|
1969/12/31|19:03:47|CXNK006B3CE8|421905047719|12.2.9.8.11|Critical|healthmgr|resource mon: LOW cpu State active|
1969/12/31|20:41:24|CXNK006B3CE8|421905047719|12.2.9.8.11|Critical|wlanmgr|QUANTENNA_INIT_FIRMWARE_LOAD_FAILED_REBOOT_QTN|
1969/12/31|20:41:25|CXNK006B3CE8|421905047719|12.2.9.8.11|Event_NORMAL|wlanmgr|power_off-qtn-device|
1969/12/31|19:00:34|CXNK006B3CE8|421905047719|12.2.9.8.11|Event_NORMAL|healthmgr|WAN's wanIfNames initialized to eth5|
1969/12/31|19:00:34|CXNK006B3CE8|421905047719|12.2.9.8.11|Event_NORMAL|healthmgr|Cold boot flag set, possible power up restart|
1969/12/31|19:01:54|CXNK006B3CE8|421905047719|12.2.9.8.11|Critical|healthmgr|resource mon: Halfway to cpu CRITICAL Thresh|
1969/12/31|19:02:20|CXNK006B3CE8|421905047719|12.2.9.8.11|Critical|healthmgr|resource mon: Halfway to cpu LOW Threshold|
1969/12/31|19:05:10|CXNK006B3CE8|421905047719|12.2.9.8.11|Critical|healthmgr|resource mon: Halfway to cpu LOW Threshold|
1969/12/31|19:09:36|CXNK006B3CE8|421905047719|12.2.9.8.11|Critical|healthmgr|resource mon: Halfway to cpu LOW Threshold|
1969/12/31|19:16:54|CXNK006B3CE8|421905047719|12.2.9.8.11|Critical|healthmgr|resource mon: Halfway to cpu LOW Threshold|
1969/12/31|19:18:26|CXNK006B3CE8|421905047719|12.2.9.8.11|Critical|healthmgr|resource mon: LOW cpu State active|
1969/12/31|20:20:45|CXNK006B3CE8|421905047719|12.2.9.8.11|Event_NORMAL|wlanmgr|qtn_client_create_success|
2020/08/03|14:18:29|CXNK006B3CE8|421905047719|12.2.9.8.11|Critical|healthmgr|resource mon: Fallback to Normal State.|
2020/08/03|14:20:23|CXNK006B3CE8|421905047719|12.2.9.8.11|Event_NORMAL|wlanmgr|QT_HOSTAPD_UP|
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|
1969/12/31|20:00:34|CXNK006B3CE8|421905047719|12.2.9.8.11|Event_NORMAL|healthmgr|WAN's wanIfNames initialized to eth5|
1969/12/31|20:00:34|CXNK006B3CE8|421905047719|12.2.9.8.11|Event_NORMAL|healthmgr|Cold boot flag set, possible power up restart|
2020/08/13|08:14:40|CXNK006B3CE8|421905047719|12.2.9.8.11|Event_NORMAL|wlanmgr|qtn_client_create_success|
2020/08/13|08:17:08|CXNK006B3CE8|421905047719|12.2.9.8.11|Event_NORMAL|wlanmgr|QT_HOSTAPD_UP|
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.

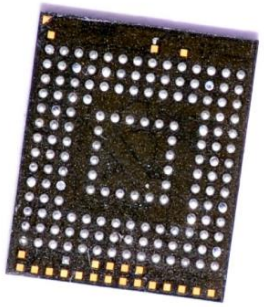
Wearables are everywhere. A first look into Huawei GT2 smartwatch

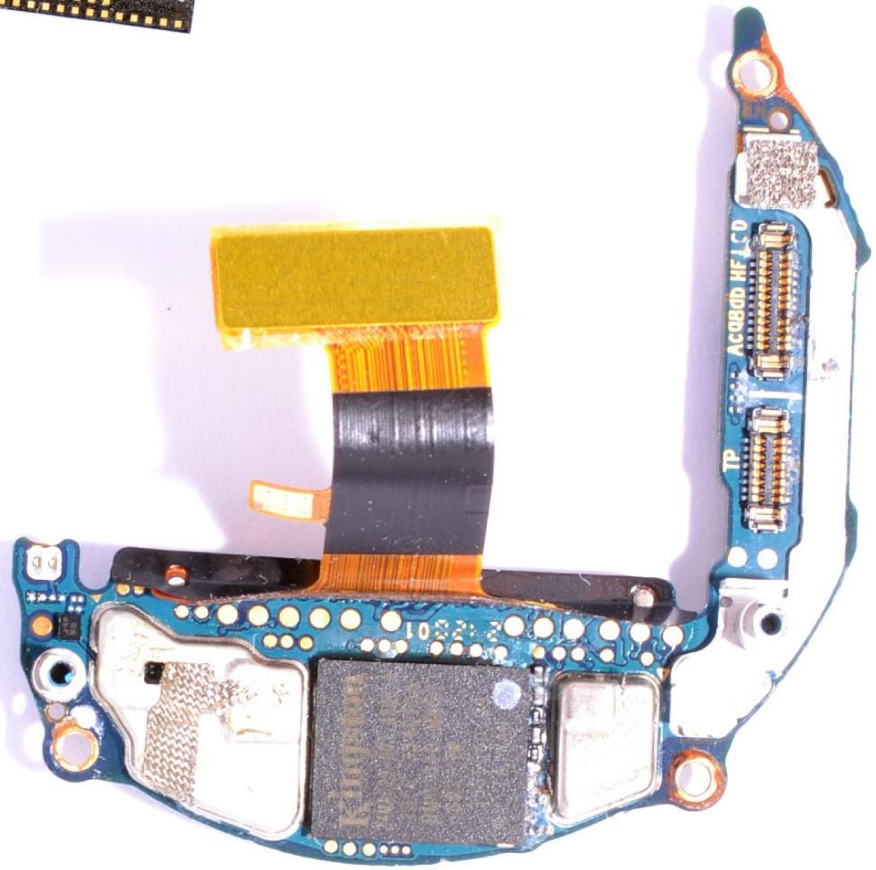
Sensor set

GPS
Bluetooth
Accelerometer sensor
Gyroscope sensor
Geomagnetic sensor
Optical heart rate sensor
Ambient light sensor
Air pressure sensor

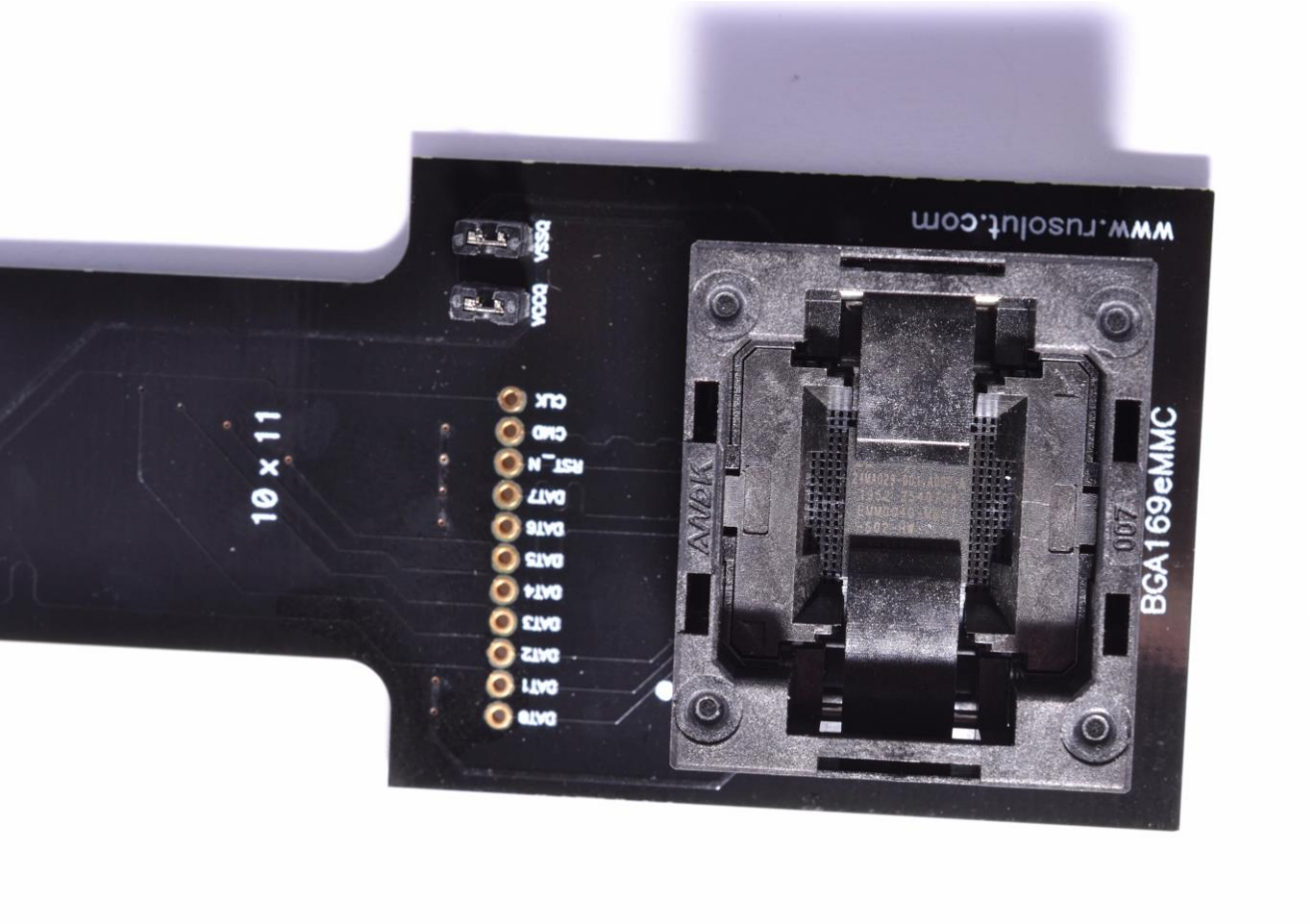


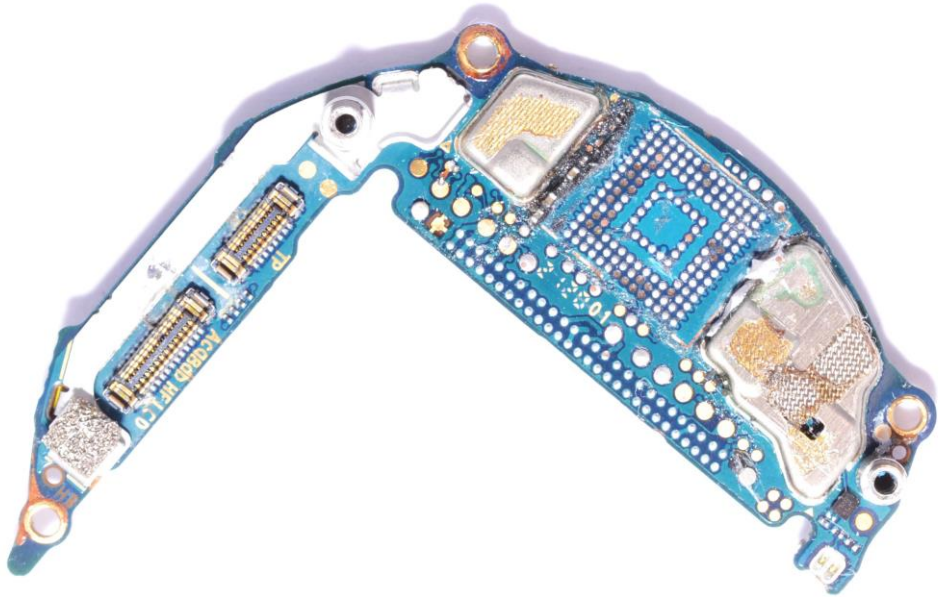
The eMMC memory chip with 4GB of space!





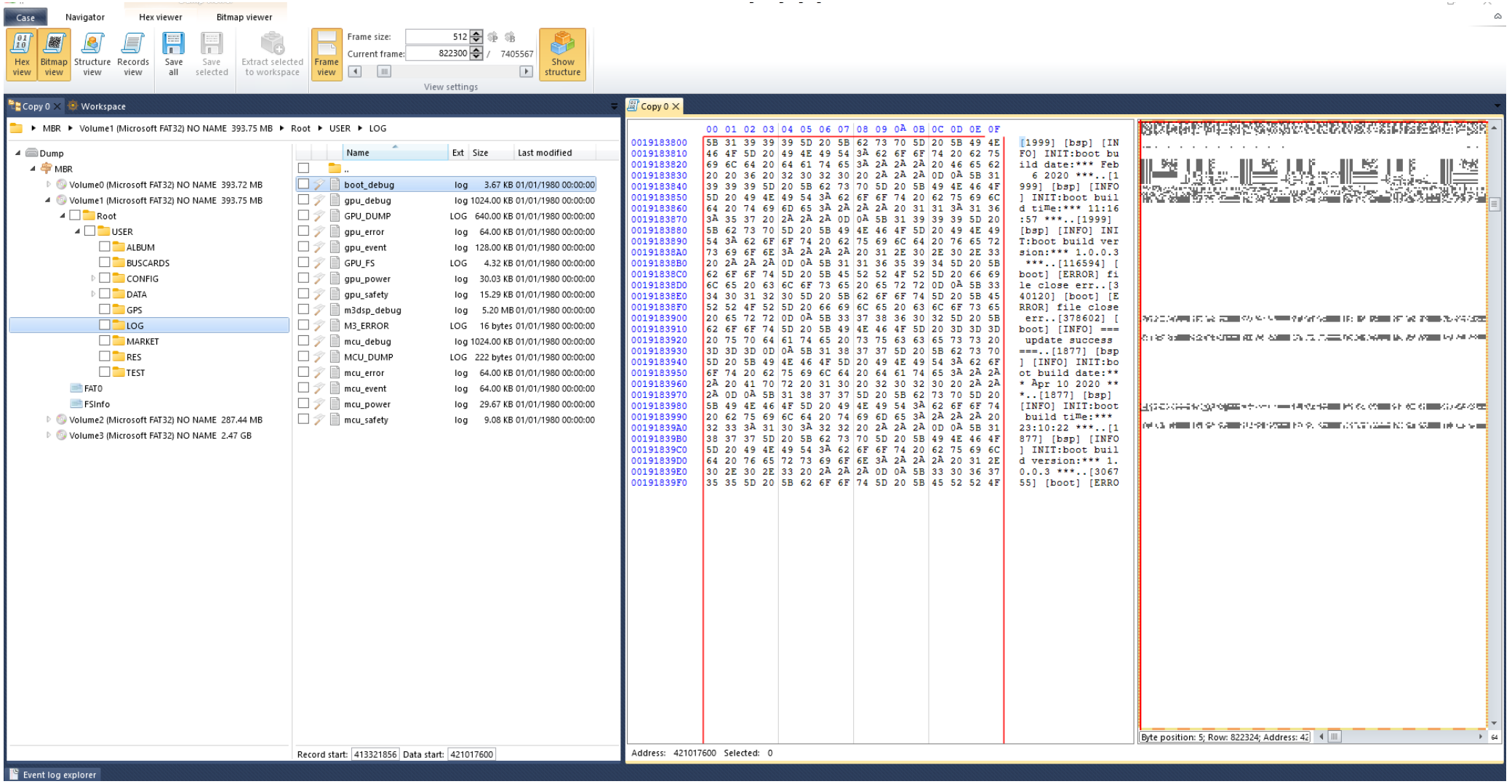
The eMMC chip is smaller that smallest one we have adapter for





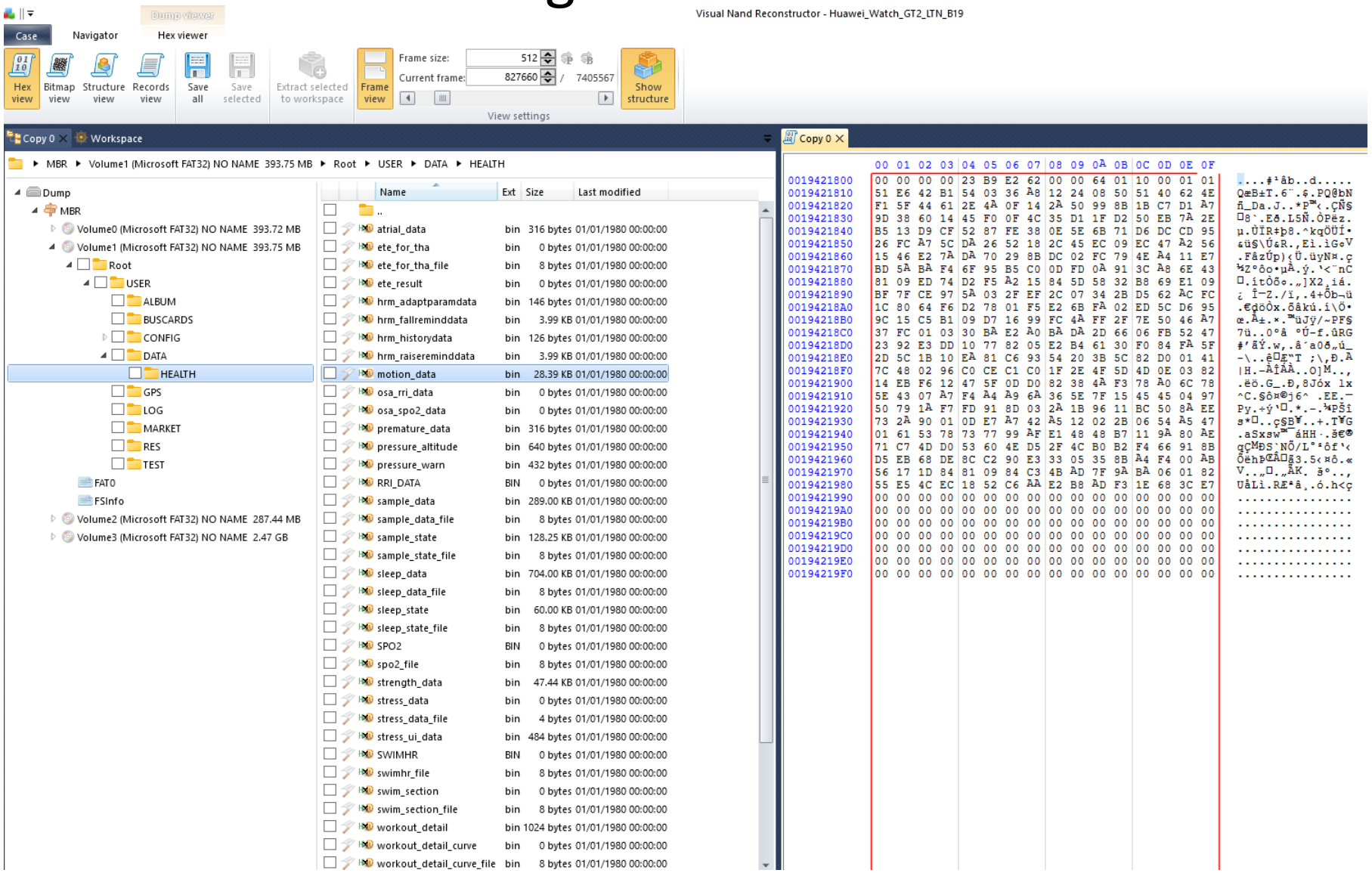
The memory had to be precisely adjusted inside the adapter for the image extraction, since only size differs but not pinout

The file system structure – multiple FAT32 volumes



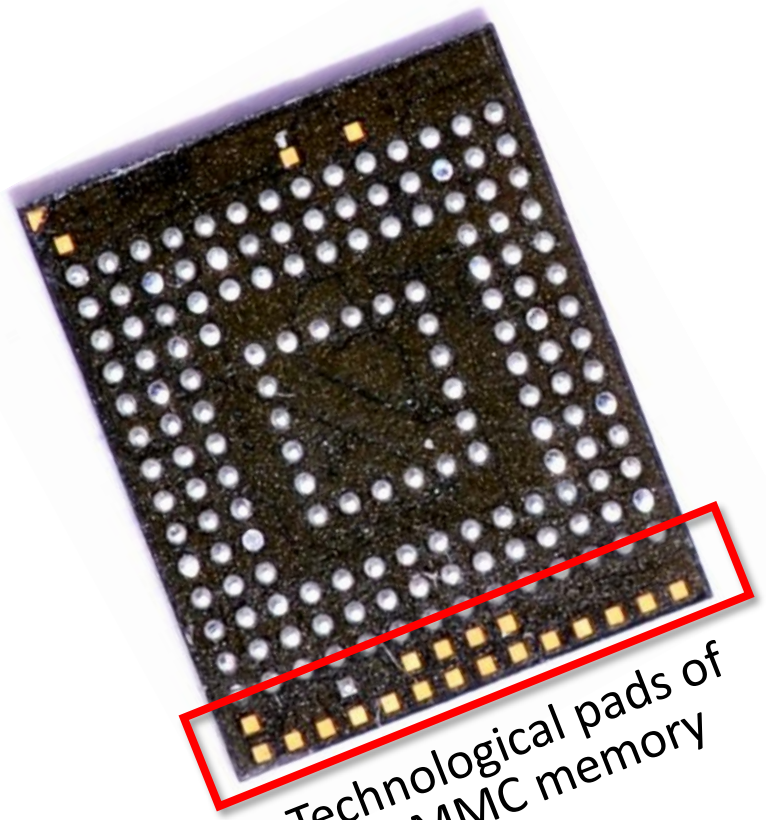
Quick analysis shows lots of logs of smartwatch boot and usage

Data storage folder was identified



Further analysis is required to pull out the readable data

Historical data access can be gained via direct NAND reading



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

Thank you!!!

www.rusolut.com

Our partner in India

3rd Eye
Techno Solutions Pvt. Ltd.
A Digital Forensics Company

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

rusolut