VEHICLE DIGITAL FORENSICS DATA ACQUISITION AND PROCESSING

Patryk Płudowski
Rusolut, Poland

rusolut

Who we are

- Vendor of data recovery and digital forensic tools:
  - Visual NAND Reconstructor
  - eMMC-NAND Reconstructor
- Leading position in flash memory data recovery and digital forensic research
- 10 years on the market
- Trained many LE agencies around the globe
- Pioneer of direct NAND data extraction of eMMC chip (bypass controller) (Link)
- Frequent speakers on various scientific and digital forensic conferences
- Published IEEE scientific paper (Link)

www.rusolut.com
Polczynska 10,
Warsaw, Poland
+48 535 054 431
info@rusolut.com

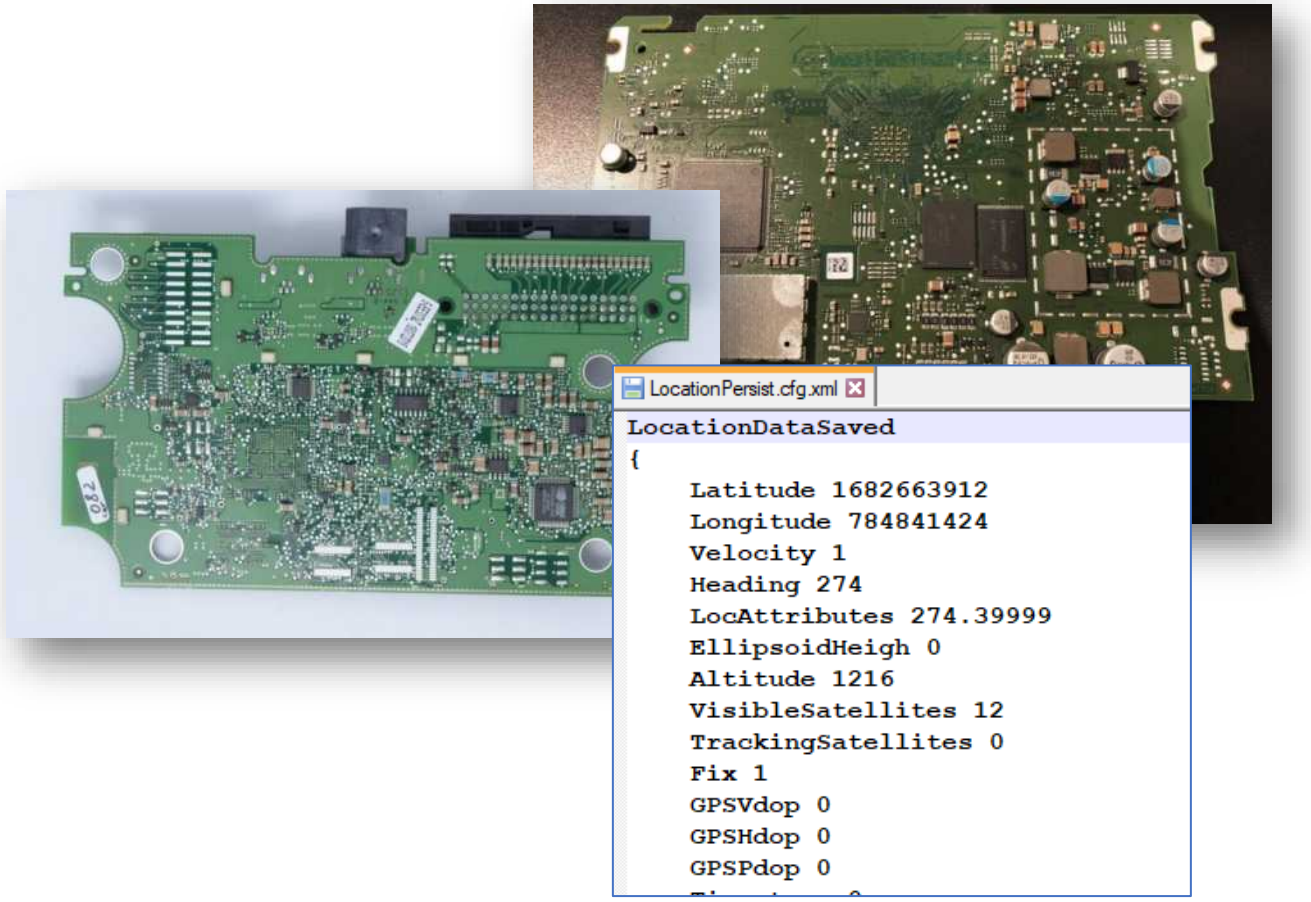
Why vehicle forensics is an important?

Infotainment systems – car related data

Every modern car has at least one data source, sometimes two or more.

Among others we have:
- Serial Number,
- VIN,
- fuel data,
- Power up and power down,
- Durations of trip,
- Radio usage…

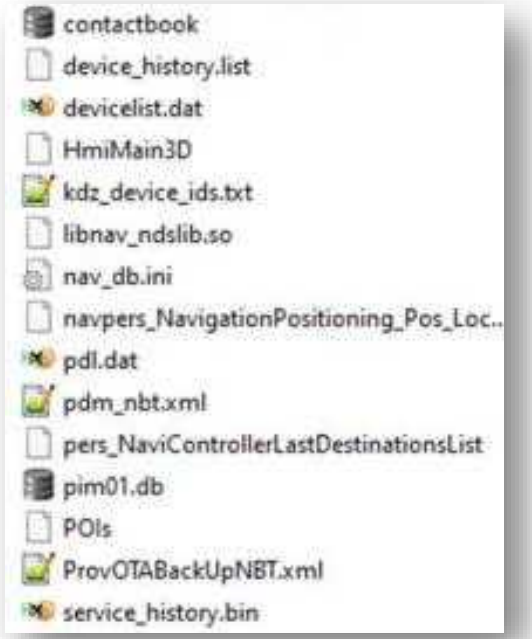
If the system supports GPS:
- destination,
- trips,
- Coordinates,
- Saved Locations…

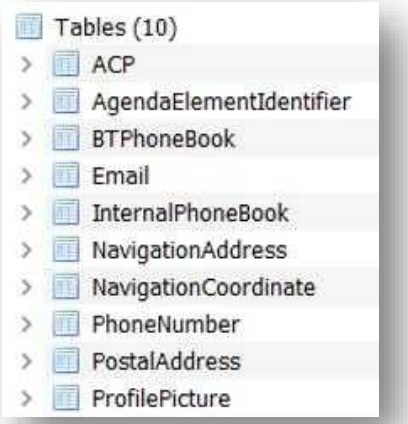


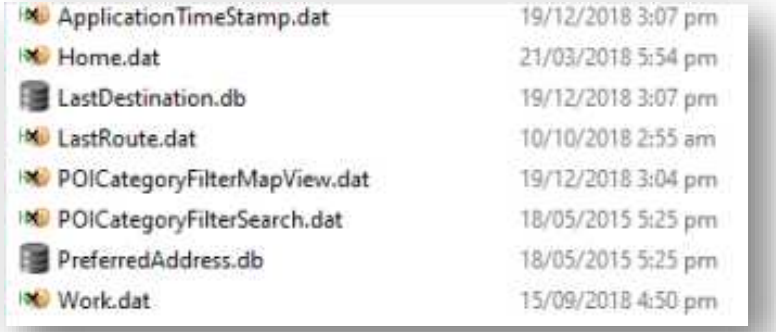
Infotainment systems – user related data

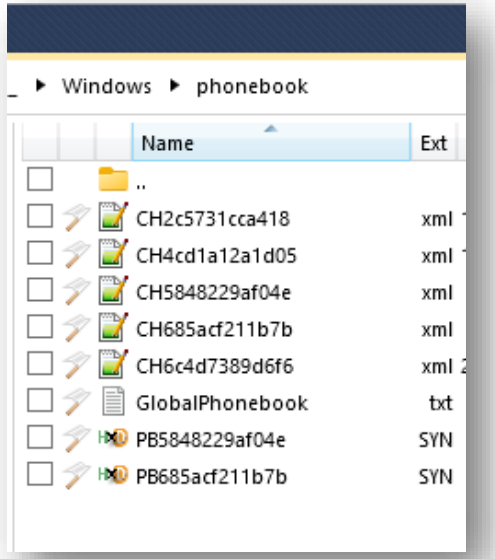
It synchronize huge amount of data from phones connected to system:

- Connection time
- phone Serial Number
- Bluetooth MAC number
- contacts book
- call logs
- sms



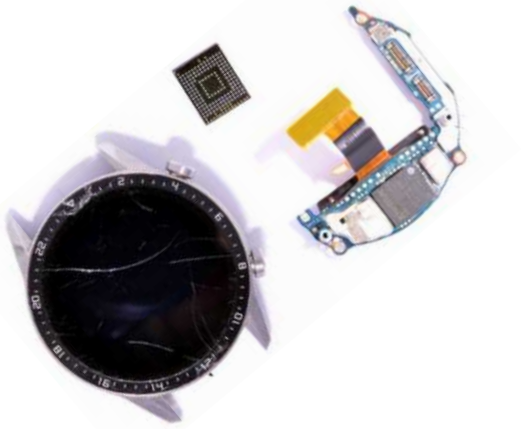


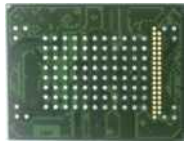


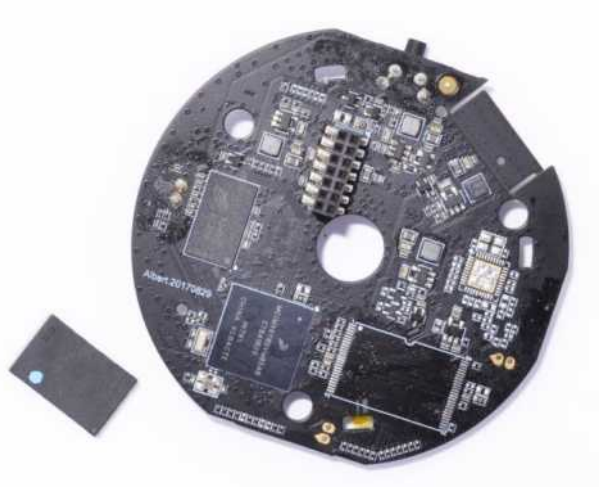


New Sources of Digital Evidence

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.**

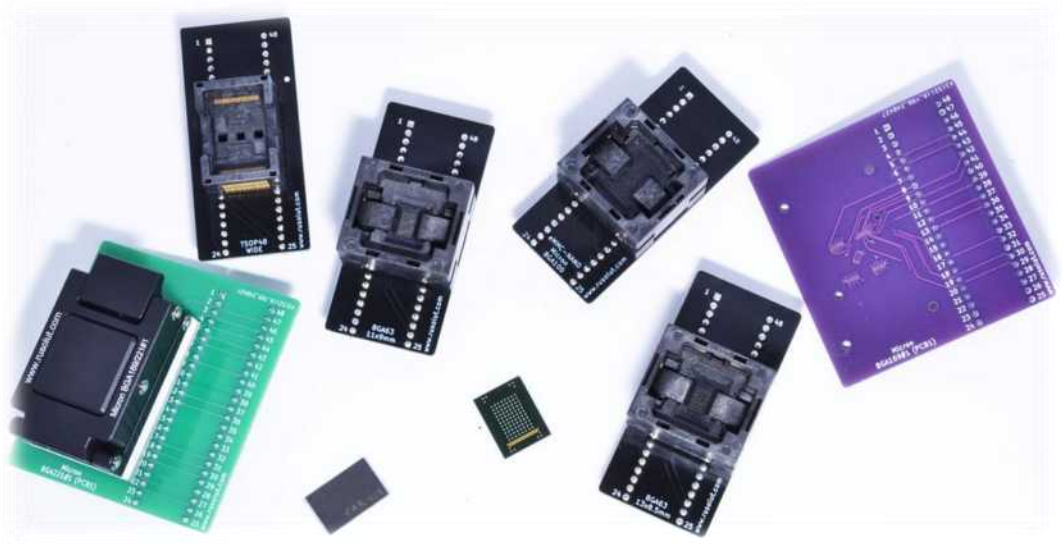




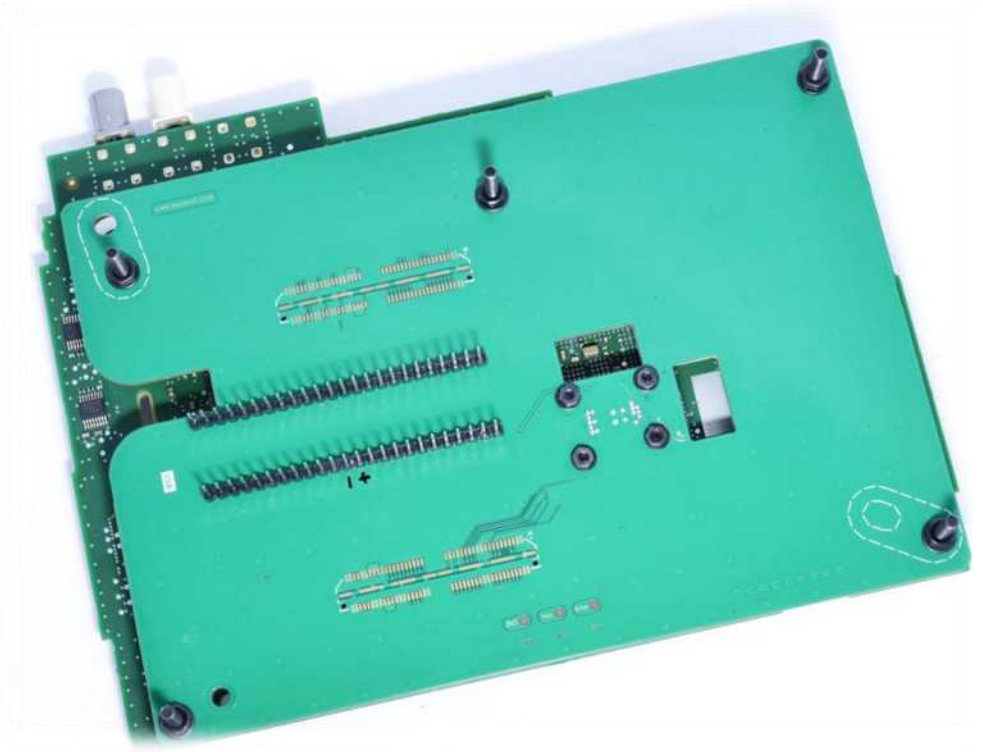


Direct methods of acquisition

Chip-off – direct read from extracted memory chip. Physically invasive method.



NEW Solderless adapters – Non invasive method of flash memory data acquisition by attaching special adapter on to system PCB.



Direct methods of acquisition

- Prevents the system from starting, keeping evidence data intact
- Works on damaged or highly damaged devices
- No risk of overwriting data and losing device logs

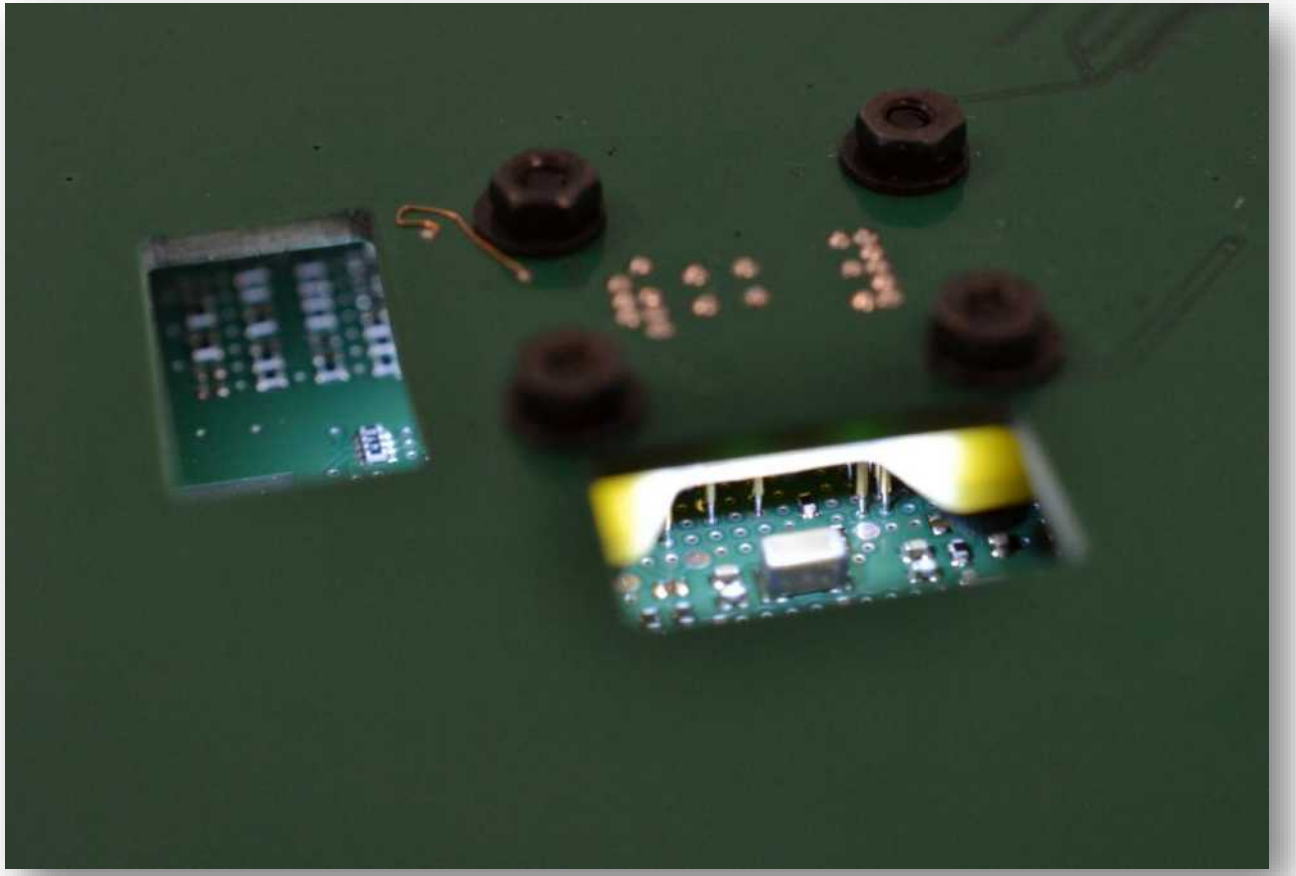
Chip-off

- Soldering/unsoldering
- Physically Invasive method
- Most universal method
- Fastest method for unknown device

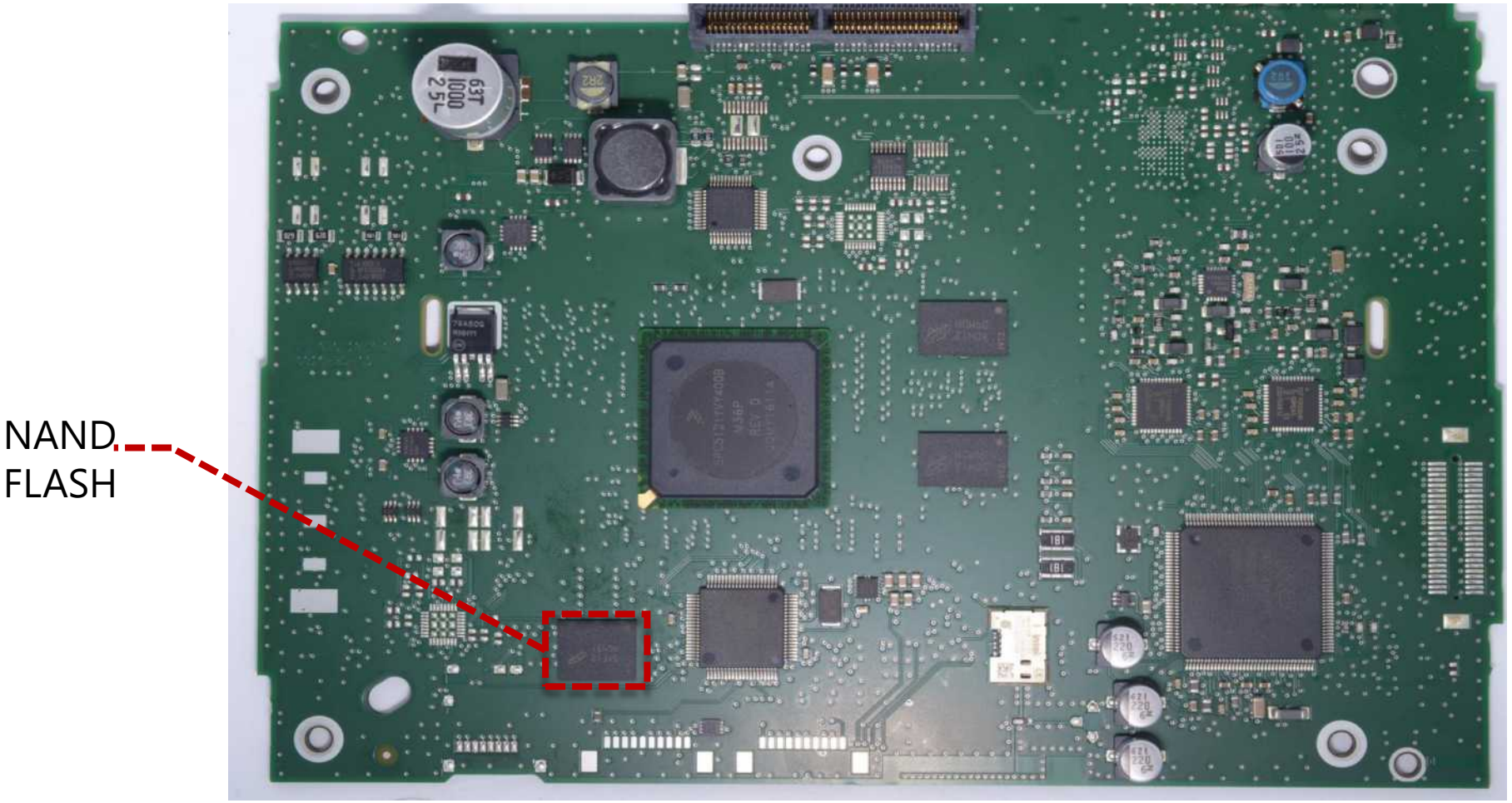
NEW Solderless adapters

- Keeps PCB of system intact
- Much safer than regular chip-off

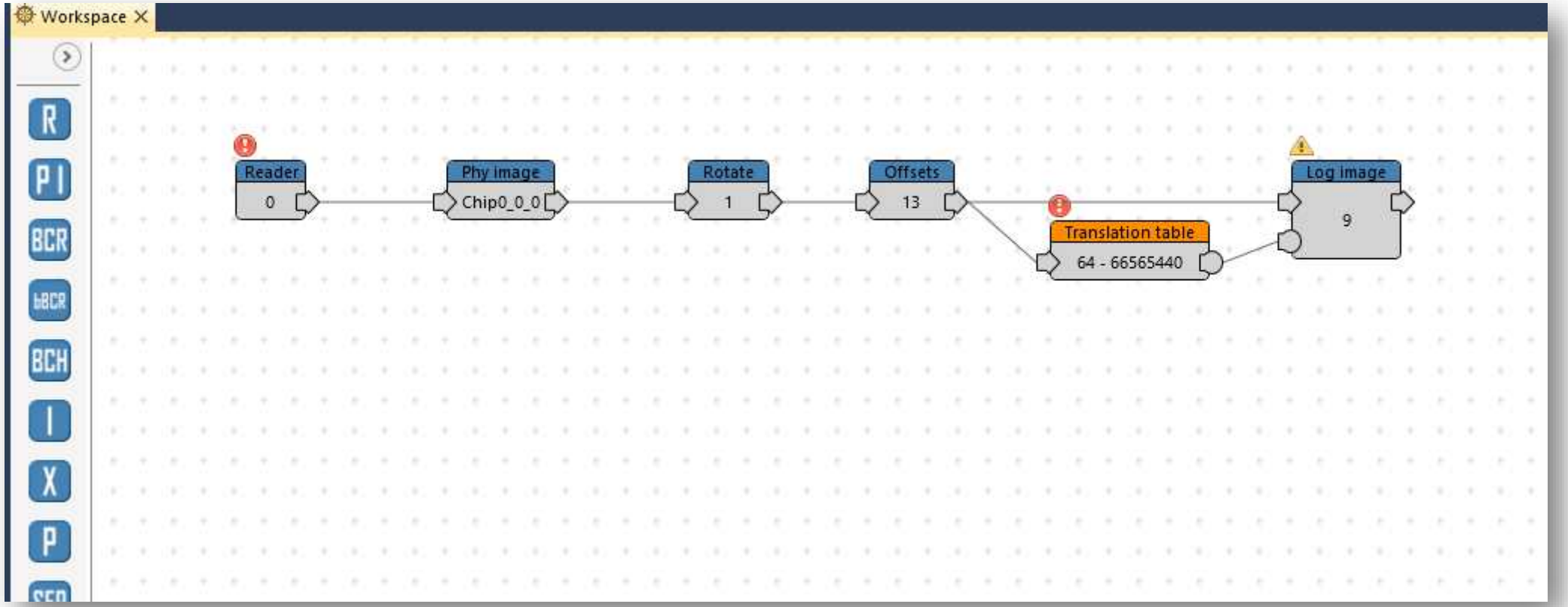
Solderless data acquisition



Peugeot 208 - real case scenario

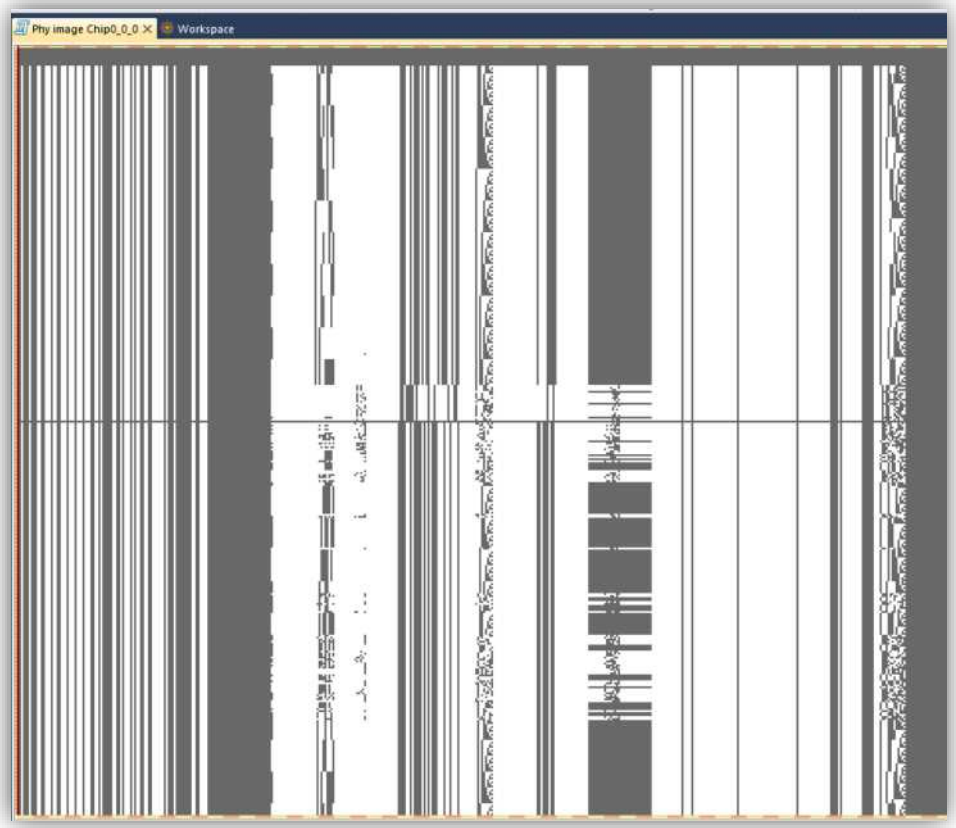


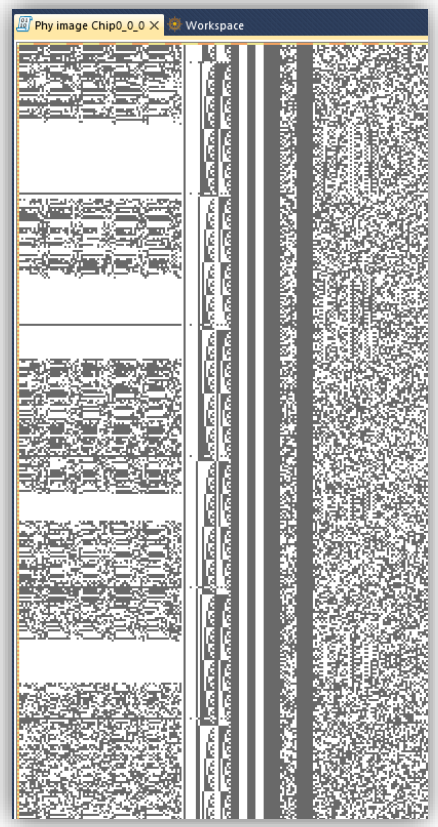
File structure reconstruction



WE CREATE A SPECIAL MODEL THAT READS DATA FROM THE MEMORY CHIP
AND TRANSFORMS IT INTO LOGICAL ORDER

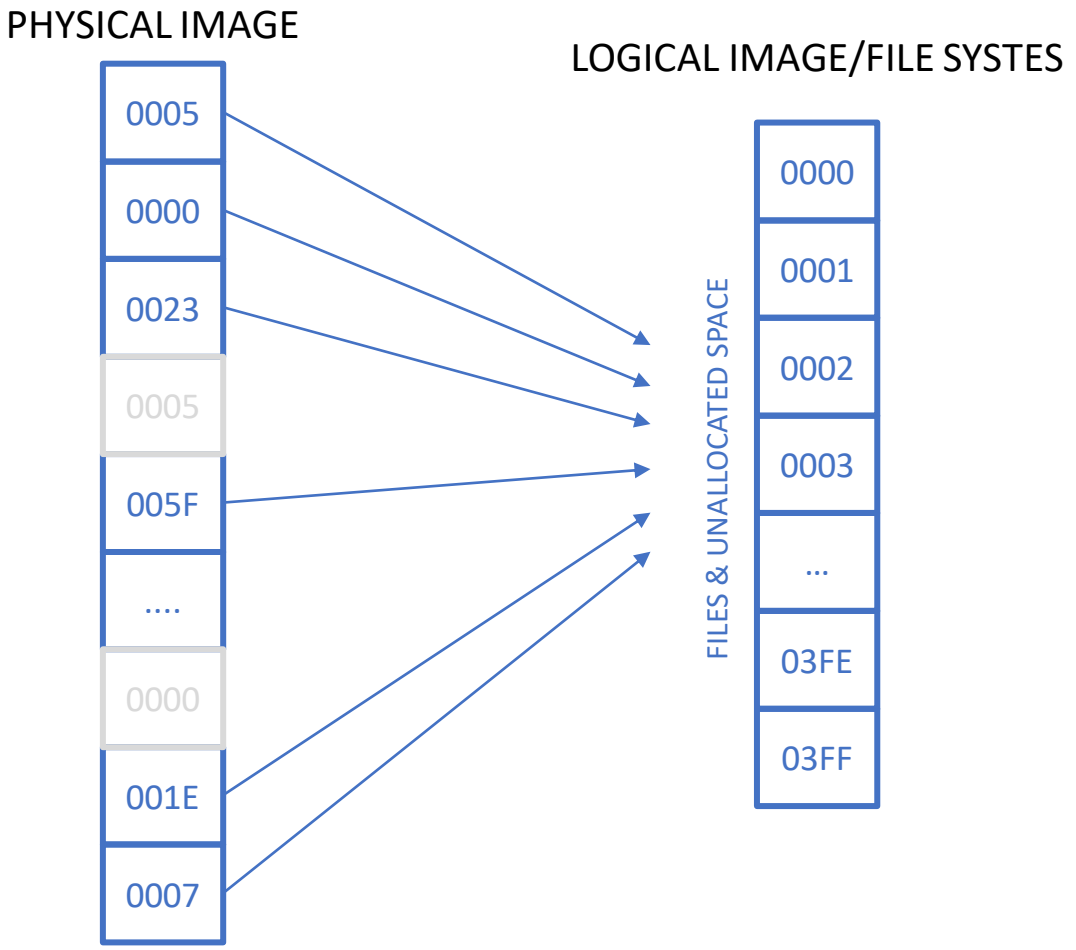
How is data in NAND memory organized? (Bitmap pattern analysis)





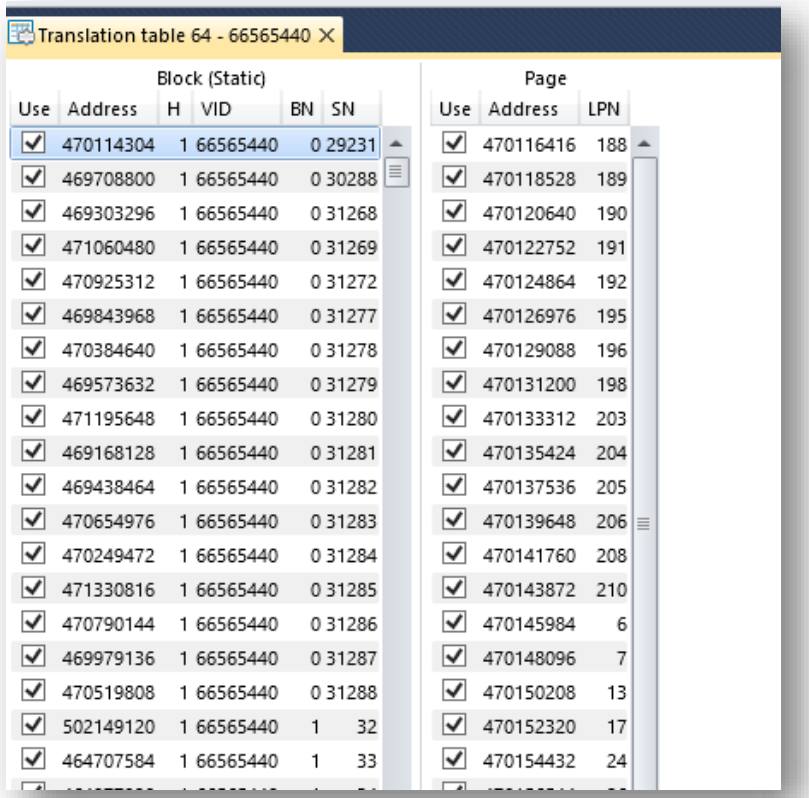
CONTROLLER WRITES DATA TO NAND MEMORY IN RANDOM ORDER
FLASH TRANSLATION LAYER IS USED TO STORE INFORMATION ABOUT THOSE PLACES

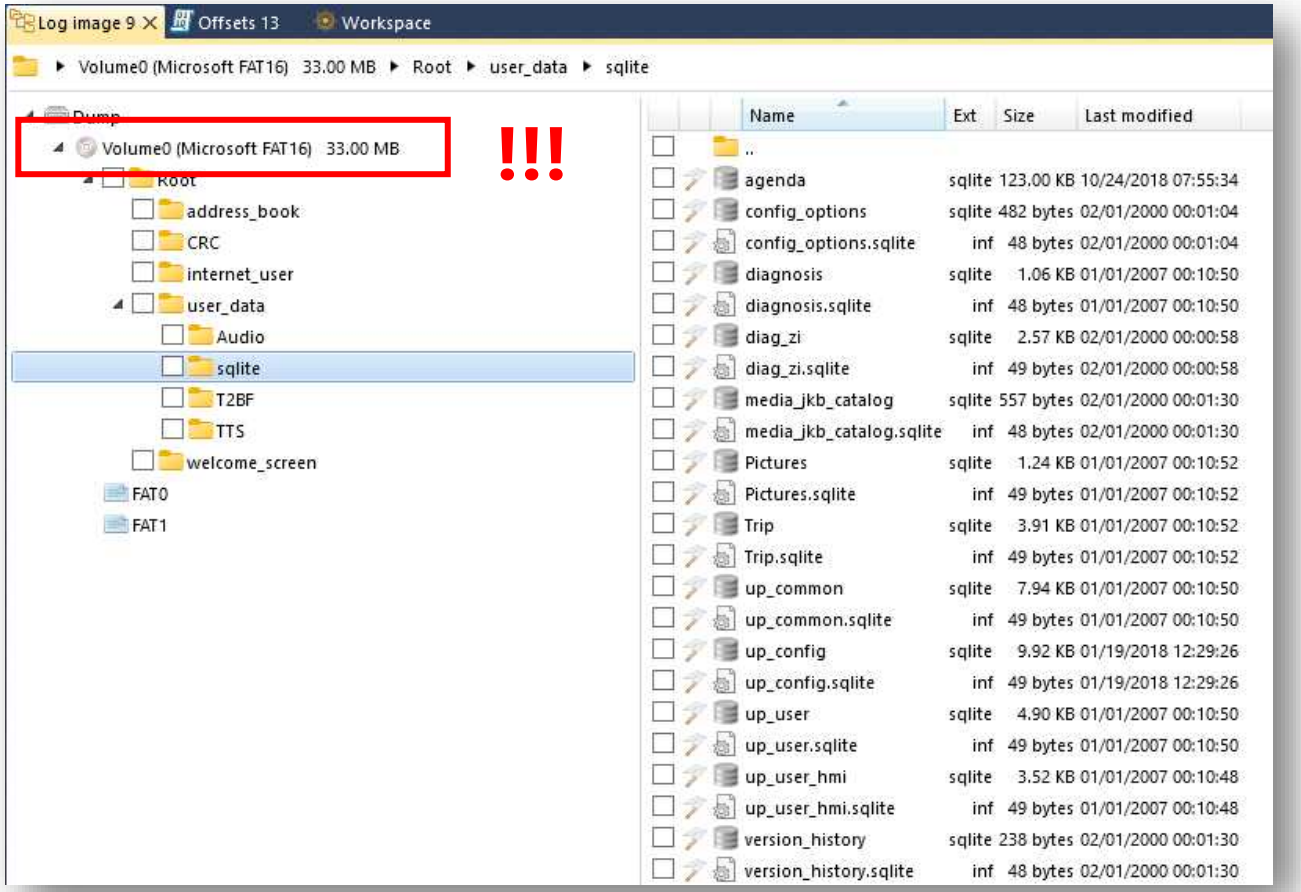
Translator - Block management



IN ORDER TO REBUILD LOGICAL DATA WE NEED TO ANALYZE FLASH TRANSLATION LAYER

Logical Image Assembly



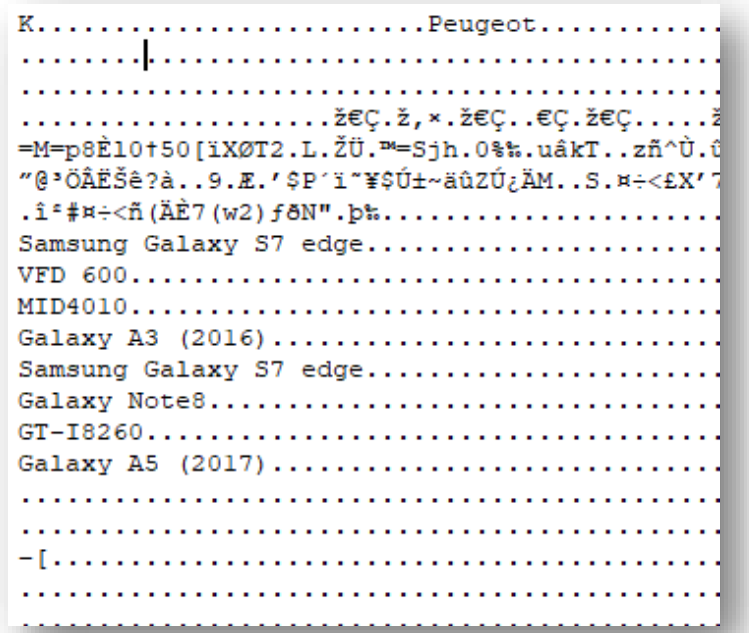


IN VNR WE CAN CREATE MODEL WITH ADVANCED TRANSLATORS

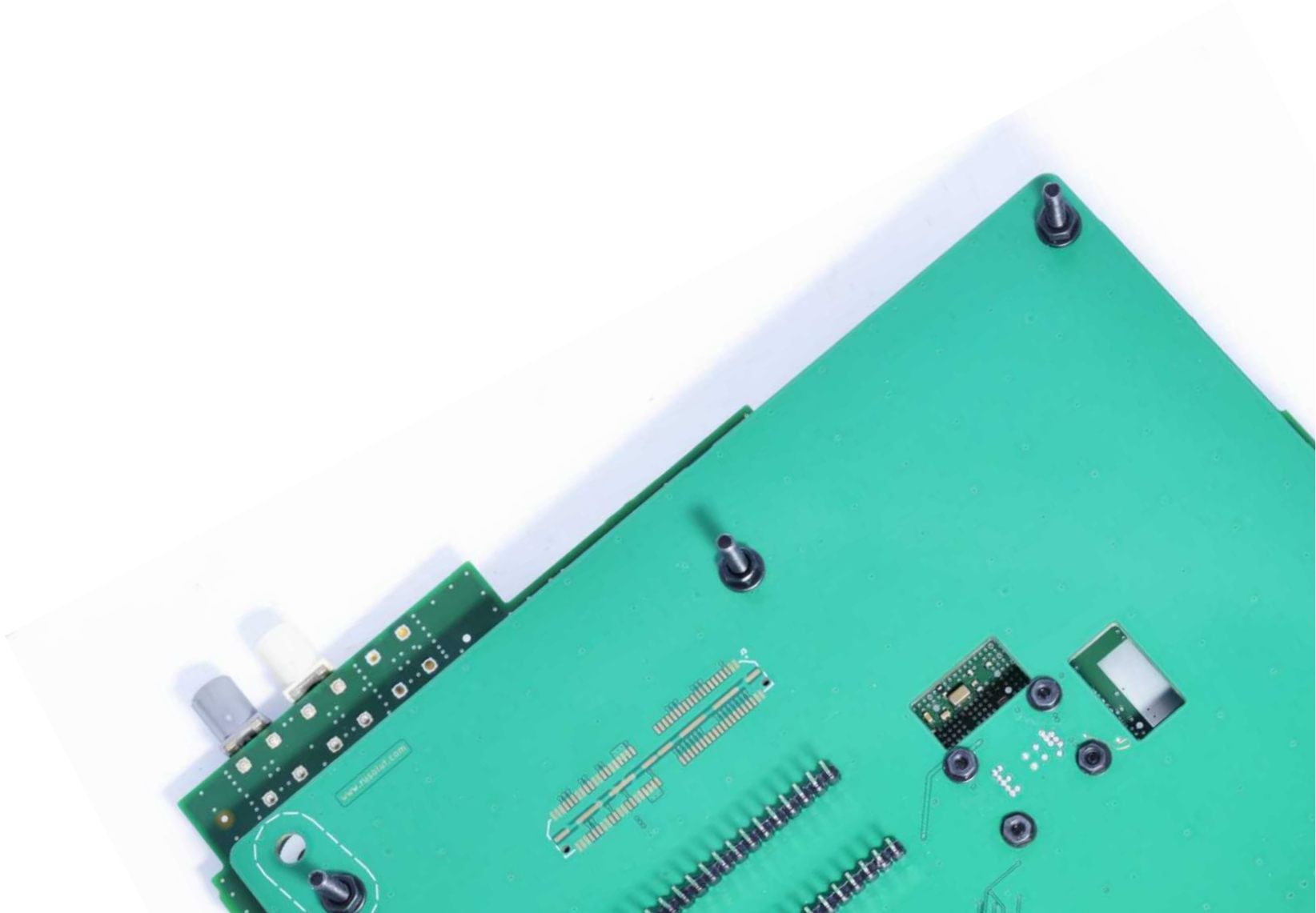
Overview of data that can be extracted

	rowid	start_mileage	end_mileage	fuel_level	start_date_time	end_date_time	star
1	5003	356585	356653	20	13/12/2022 10:42:00	13/12/2022 10:53:00	
2	5023	357454	357542	86	16/12/2022 09:46:00	16/12/2022 09:58:00	
3	5024	357542	357611	84	16/12/2022 10:12:00	16/12/2022 10:24:00	
4	5027	357768	358028	78	18/12/2022 16:04:00	18/12/2022 16:32:00	
5	5028	358028	358055	78	18/12/2022 16:50:00	18/12/2022 16:56:00	
6	5029	358055	358059	77	18/12/2022 18:31:00	18/12/2022 18:33:00	
7	5030	358059	358306	74	18/12/2022 19:03:00	18/12/2022 19:28:00	
8	5031	358306	358375	73	19/12/2022 07:41:00	19/12/2022 08:07:00	
9	5032	358375	358458	72	19/12/2022 08:12:00	19/12/2022 08:24:00	
10	5033	358458	358475	72	19/12/2022 08:38:00	19/12/2022 08:41:00	
11	5033	358458	358475	72	19/12/2022 08:38:00	19/12/2022 08:41:00	
12	5034	358475	358492	72	19/12/2022 08:42:00	19/12/2022 08:45:00	
13	5034	358475	358492	72	19/12/2022 08:42:00	19/12/2022 08:45:00	
14	5035	358492	358526	71	19/12/2022 14:03:00	19/12/2022 14:12:00	
15	5035	358492	358526	71	19/12/2022 14:03:00	19/12/2022 14:12:00	
16	5036	358526	358592	70	19/12/2022 14:16:00	19/12/2022 14:27:00	
17	5036	358526	358592	70	19/12/2022 14:16:00	19/12/2022 14:27:00	
18	5037	358592	358601	70	19/12/2022 14:33:00	19/12/2022 14:37:00	
19	5037	358592	358601	70	19/12/2022 14:33:00	19/12/2022 14:37:00	
20	5038	358601	358603	69	19/12/2022 14:40:00	19/12/2022 14:41:00	
21	5038	358601	358603	69	19/12/2022 14:40:00	19/12/2022 14:41:00	
22	5039	358603	358673	69	19/12/2022 14:43:00	19/12/2022 14:56:00	
23	5039	358603	358673	69	19/12/2022 14:43:00	19/12/2022 14:56:00	

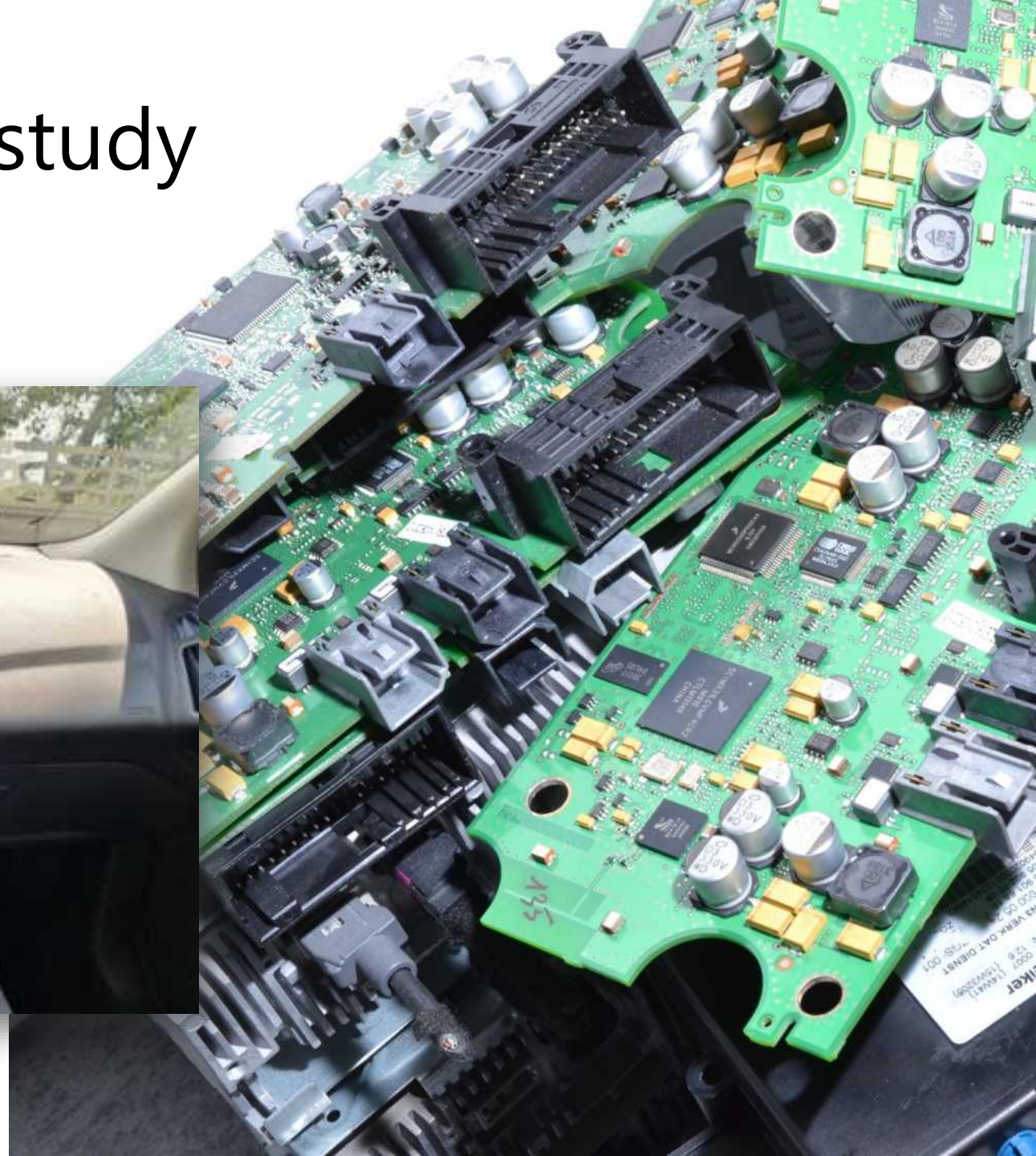
Total: 117



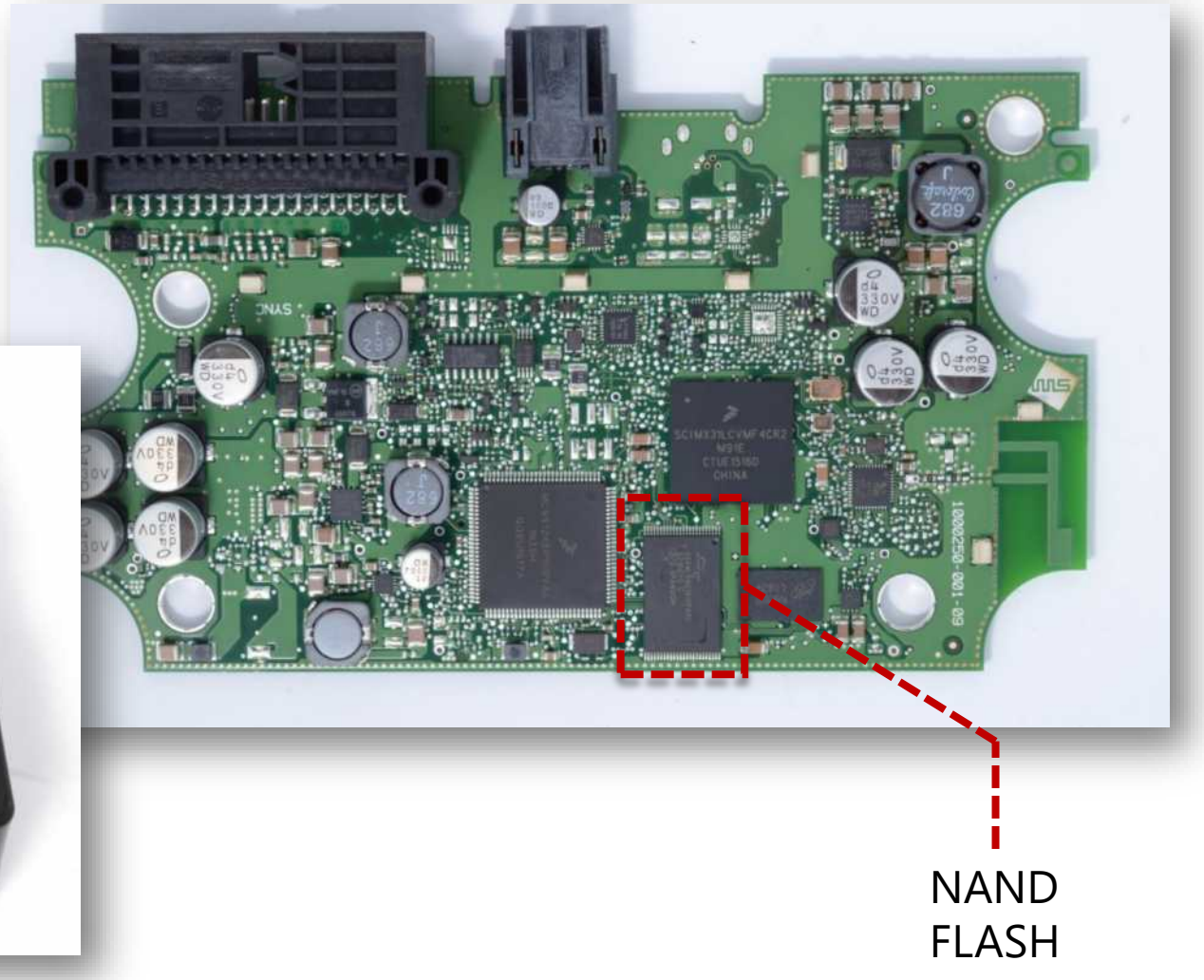
Hands on case study – live demo



Ford Sync – case study



Ford Sync – user data overview

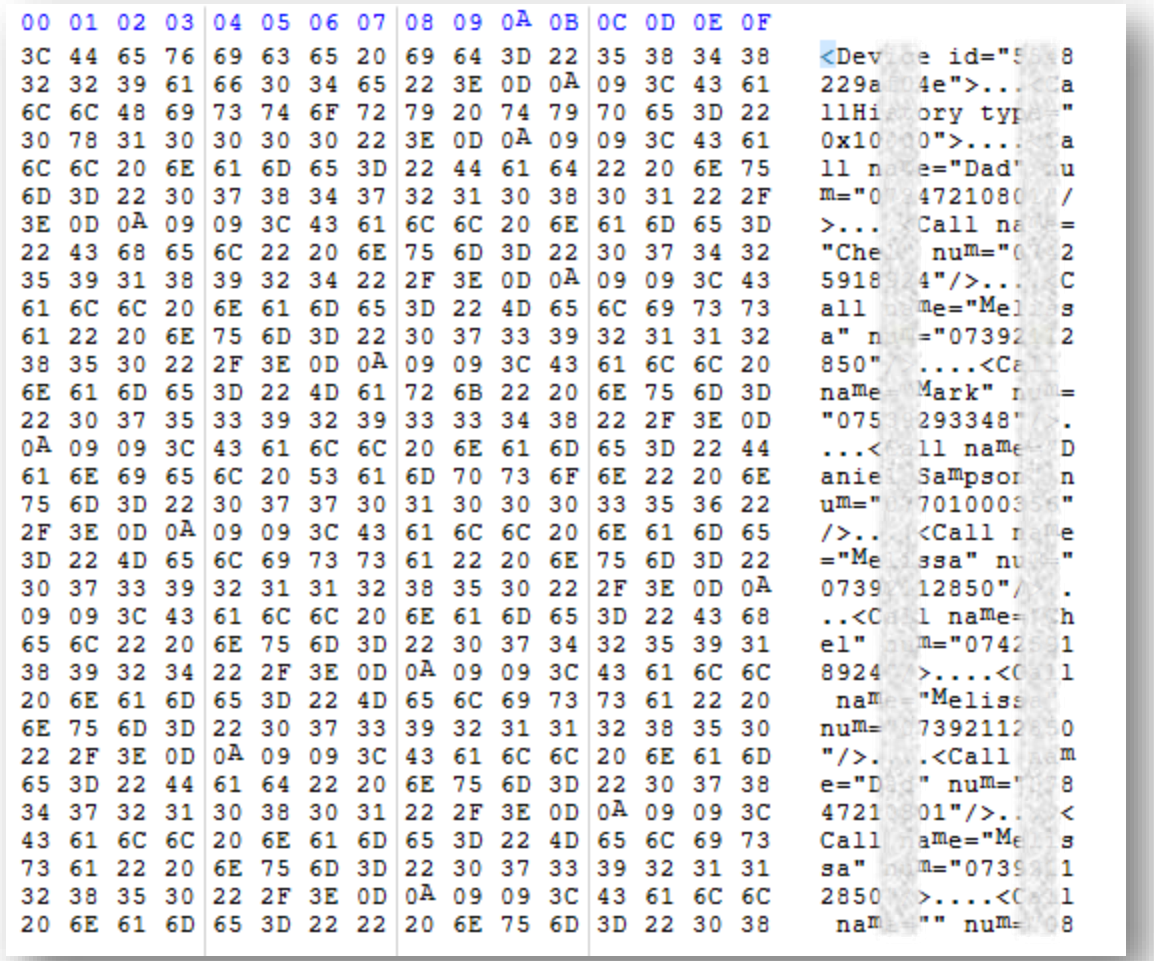


List of connected devices

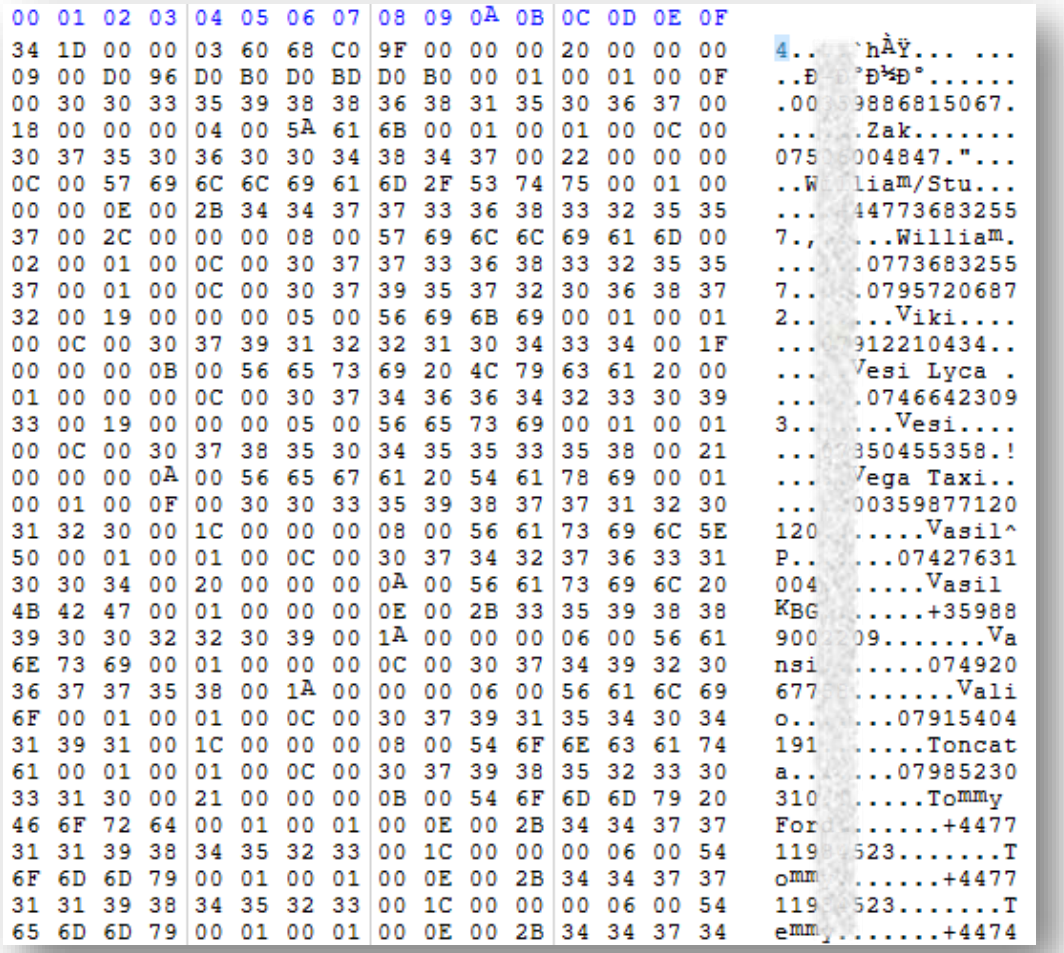
```
9805 >>>> Paired devices(0x00000007):
9807    device: 3. [David's iPhone] [0x0000c88 a312], active = 0, primary = 1,
9818    device: 5. [Bawbags ipod] [0x0000d8d1c d0], active = 0, primary = 0, pa
9829    device: 4. [JULES JUKE BOX] [0x00002cf 27d], active = 0, primary = 0,
9840    device: 2. [D2303] [0x000044d4e0ba5071 tive = 0, primary = 0, pairorder
9850    device: 1. [BAWBAG] [0x0000bccfccefb4c tive = 0, primary = 0, pairorde
```

```
1669825 MPCoreDump: Index #0, Device id [name:JULES JUKE BOX][serial:CCQ
1669833 MPCoreDump: Type = Persisted. , Src Id 0, Port 1, State 0x11
1669840 MPCoreDump: DeviceId: [name:JULES JUKE BOX][serial:CCQN ][protocol:6
1669847 MPCoreDump: Index #1, Device id [name:David's iPhone][serial:DNQ
1669856 MPCoreDump: Type = Persisted. , Src Id 1, Port 1, State 0x11
1669862 MPCoreDump: DeviceId: [name:David's iPhone][serial:DNQ ][protocol:6
1669870 MPCoreDump: Index #2, Device id LineIn.
1669874 MPCoreDump: Type = Command/Control. , Src Id 2, Port 4, State 0x4, LastAcce
1669882 MPCoreDump: DeviceId: LineIn
1669885 MPCoreDump: Index #3, Device id d8d1 .
1669890 MPCoreDump: Type = Persisted. , Src Id 3, Port 3, State 0x11
1669896 MPCoreDump: DeviceId: d8d1
1669900 MPCoreDump: Index #4, Device id [name:David s iPhone][serial:F17
1669909 MPCoreDump: Type = Persisted. , Src Id 4, Port 1, State 0x11
1669915 MPCoreDump: DeviceId: [name:David s iPhone][serial:F17 ][protocol:6
1669923 MPCoreDump: Index #5, Device id [model:HTC Desire X][manufacturer:HTC][vers
1669934 MPCoreDump: Type = Persisted. , Src Id 5, Port 1, State 0x54
1669940 MPCoreDump: DeviceId: [model:HTC Desire X][manufacturer:HTC][version:2.22.2
```

Call log and phone book

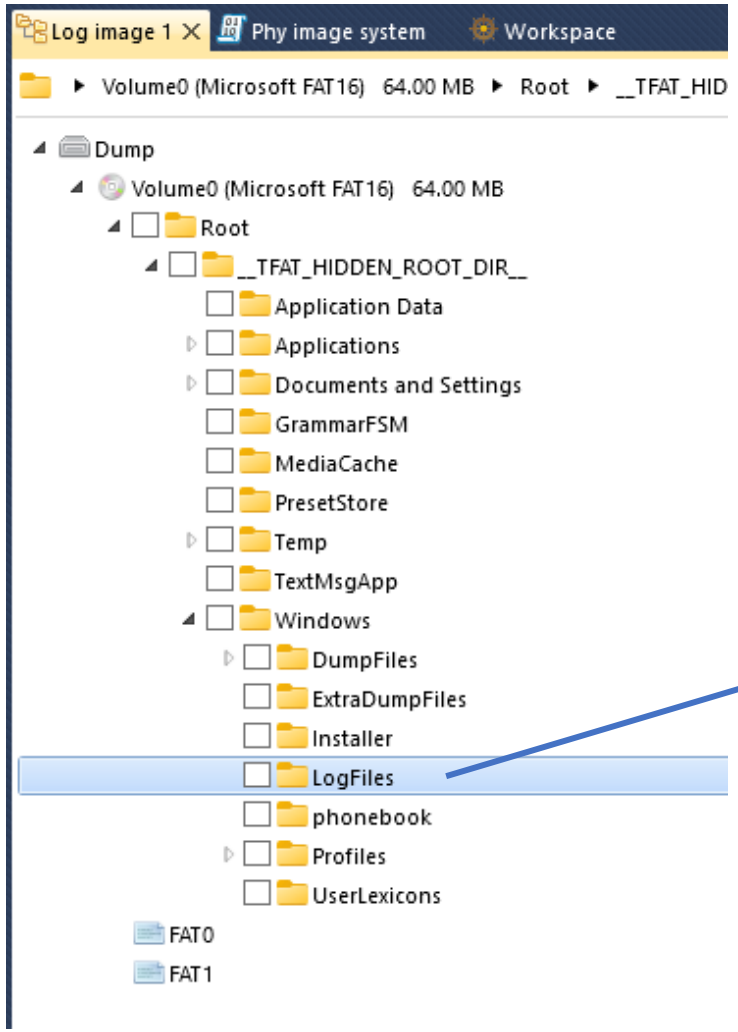


```
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
3C 44 65 76 69 63 65 20 69 64 3D 22 35 38 34 38   <Dev e id="5  8
32 32 39 61 66 30 34 65 22 3E 0D 0A 09 3C 43 61   229a 4e">...  a
6C 6C 48 69 73 74 6F 72 79 20 74 79 70 65 3D 22   llHi ory typ  "
30 78 31 30 30 30 30 22 3E 0D 0A 09 09 3C 43 61   0x10 0">....  a
6C 6C 20 6E 61 6D 65 3D 22 44 61 64 22 20 6E 75   ll n e="Dad"  u
6D 3D 22 30 37 38 34 37 32 31 30 38 30 31 22 2F   m="0 4721080  /
3E 0D 0A 09 09 3C 43 61 6C 6C 20 6E 61 6D 65 3D   >...  Call na  =
22 43 68 65 6C 22 20 6E 75 6D 3D 22 30 37 34 32   "Che  nu="(  2
35 39 31 38 39 32 34 22 2F 3E 0D 0A 09 09 3C 43   5918 4"/>...  C
61 6C 6C 20 6E 61 6D 65 3D 22 4D 65 6C 69 73 73   all  me="Mel  s
61 22 20 6E 75 6D 3D 22 30 37 33 39 32 31 31 32   a" n ="07392  2
38 35 30 22 2F 3E 0D 0A 09 09 3C 43 61 6C 6C 20   850" ....<Ca
6E 61 6D 65 3D 22 4D 61 72 6B 22 20 6E 75 6D 3D   name Mark" n  =
22 30 37 35 33 39 32 39 33 33 34 38 22 2F 3E 0D   "075 293348"  .
0A 09 09 3C 43 61 6C 6C 20 6E 61 6D 65 3D 22 44   ...< ll name  D
61 6E 69 65 6C 20 53 61 6D 70 73 6F 6E 22 20 6E   anie Sampson  n
75 6D 3D 22 30 37 37 30 31 30 30 30 33 35 36 22   um="  7010003  "
2F 3E 0D 0A 09 09 3C 43 61 6C 6C 20 6E 61 6D 65   />..  <Call n  e
3D 22 4D 65 6C 69 73 73 61 22 20 6E 75 6D 3D 22   ="Me ssa" nu  "
30 37 33 39 32 31 31 32 38 35 30 22 2F 3E 0D 0A   0739 12850"/  .
09 09 3C 43 61 6C 6C 20 6E 61 6D 65 3D 22 43 68   ..<C l name=  h
65 6C 22 20 6E 75 6D 3D 22 30 37 34 32 35 39 31   el"  m="0742  1
38 39 32 34 22 2F 3E 0D 0A 09 09 3C 43 61 6C 6C   8924 >....<C  l
20 6E 61 6D 65 3D 22 4D 65 6C 69 73 73 61 22 20    nam "Meliss
6E 75 6D 3D 22 30 37 33 39 32 31 31 32 38 35 30   num= 7392112  0
22 2F 3E 0D 0A 09 09 3C 43 61 6C 6C 20 6E 61 6D   "/>.  .<Call  m
65 3D 22 44 61 64 22 20 6E 75 6D 3D 22 30 37 38   e="D " num="  8
34 37 32 31 30 38 30 31 22 2F 3E 0D 0A 09 09 3C   4721 01"/>..  <
43 61 6C 6C 20 6E 61 6D 65 3D 22 4D 65 6C 69 73   Call ame="Me  s
73 61 22 20 6E 75 6D 3D 22 30 37 33 39 32 31 31   sa"  m="0739  1
32 38 35 30 22 2F 3E 0D 0A 09 09 3C 43 61 6C 6C   2850 >....<C  l
20 6E 61 6D 65 3D 22 22 20 6E 75 6D 3D 22 30 38    nam "" num=  8
```



```
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
34 1D 00 00 03 60 68 C0 9F 00 00 00 20 00 00 00   4....`hÀŸ... ...
09 00 D0 96 D0 B0 D0 BD D0 B0 00 01 00 01 00 0F   ..Ð– Ð°Ð½Ð°......
00 30 30 33 35 39 38 38 36 38 31 35 30 36 37 00   .00 9886815067.
18 00 00 00 04 00 5A 61 6B 00 01 00 01 00 0C 00   ......Zak.......
30 37 35 30 36 30 30 34 38 34 37 00 22 00 00 00   075 004847."...
0C 00 57 69 6C 6C 69 61 6D 2F 53 74 75 00 01 00   ..W liam/Stu...
00 00 0E 00 2B 34 34 37 37 33 36 38 33 32 35 35   ... 44773683255
37 00 2C 00 00 00 08 00 57 69 6C 6C 69 61 6D 00   7.,  ...William.
02 00 01 00 0C 00 30 37 37 33 36 38 33 32 35 35   ... .0773683255
37 00 01 00 0C 00 30 37 39 35 37 32 30 36 38 37   7.. .0795720687
32 00 19 00 00 00 05 00 56 69 6B 69 00 01 00 01   2.. ...Viki....
00 0C 00 30 37 39 31 32 32 31 30 34 33 34 00 1F   ... 912210434..
00 00 00 0B 00 56 65 73 69 20 4C 79 63 61 20 00   ... Vesi Lyca .
01 00 00 00 0C 00 30 37 34 36 36 34 32 33 30 39   ... .0746642309
33 00 19 00 00 00 05 00 56 65 73 69 00 01 00 01   3.. ...Vesi....
00 0C 00 30 37 38 35 30 34 35 35 33 35 38 00 21   ... 350455358.!
00 00 00 0A 00 56 65 67 61 20 54 61 78 69 00 01   ... Vega Taxi..
00 01 00 0F 00 30 30 33 35 39 38 37 37 31 32 30   ... 00359877120
31 32 30 00 1C 00 00 00 08 00 56 61 73 69 6C 5E   120 .....Vasil^
50 00 01 00 01 00 0C 00 30 37 34 32 37 36 33 31   P.. ...07427631
30 30 34 00 20 00 00 00 0A 00 56 61 73 69 6C 20   004 .....Vasil
4B 42 47 00 01 00 00 00 0E 00 2B 33 35 39 38 38   KBG .....+35988
39 30 30 32 32 30 39 00 1A 00 00 00 06 00 56 61   900 09.......Va
6E 73 69 00 01 00 00 00 0C 00 30 37 34 39 32 30   nsi .....074920
36 37 37 35 38 00 1A 00 00 00 06 00 56 61 6C 69   677 .......Vali
6F 00 01 00 01 00 0C 00 30 37 39 31 35 34 30 34   o.. ...07915404
31 39 31 00 1C 00 00 00 08 00 54 6F 6E 63 61 74   191 .....Toncat
61 00 01 00 01 00 0C 00 30 37 39 38 35 32 33 30   a.. ...07985230
33 31 30 00 21 00 00 00 0B 00 54 6F 6D 6D 79 20   310 .....Tommy
46 6F 72 64 00 01 00 01 00 0E 00 2B 34 34 37 37   For .....+4477
31 31 39 38 34 35 32 33 00 1C 00 00 00 06 00 54   119 523.......T
6F 6D 6D 79 00 01 00 01 00 0E 00 2B 34 34 37 37   omm .....+4477
31 31 39 38 34 35 32 33 00 1C 00 00 00 06 00 54   119 523.......T
65 6D 6D 79 00 01 00 01 00 0E 00 2B 34 34 37 34   emm .....+4474
```

Navigation data of the vehicle

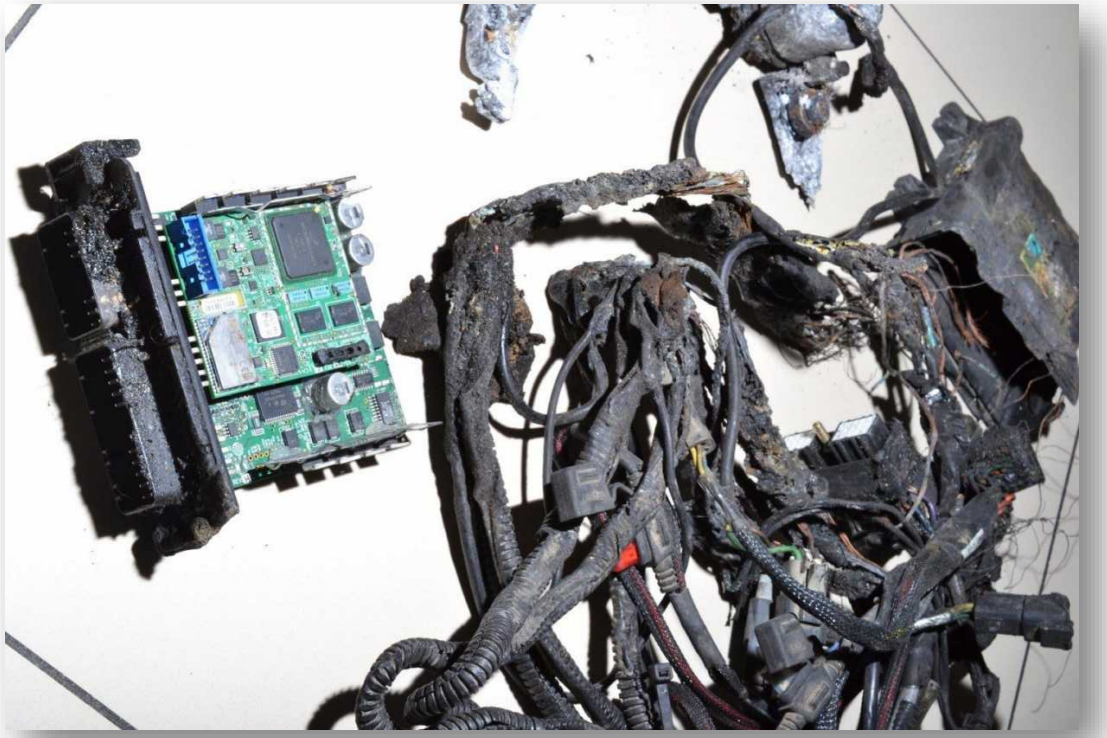


Car stores data in various places. We need to analyze them in order to get as much data as possible

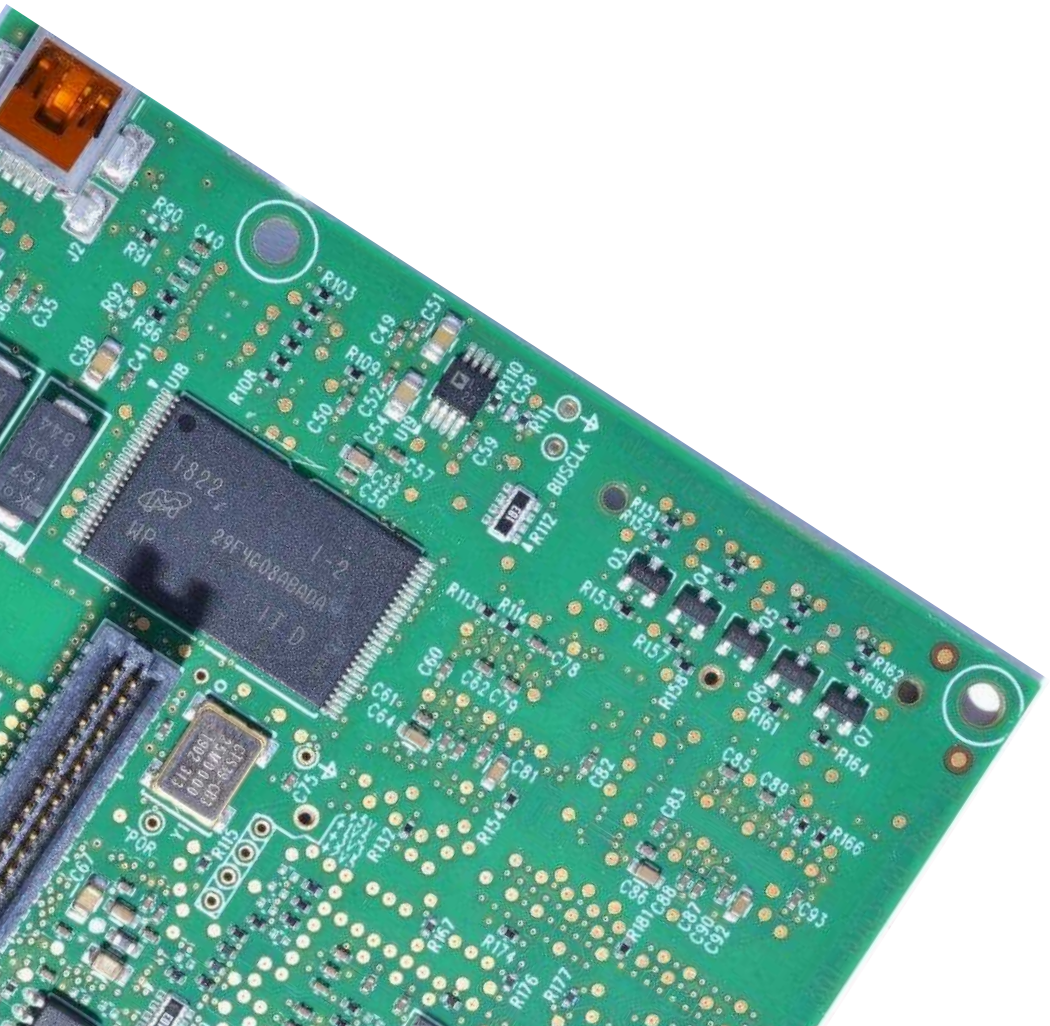
51°49'51.9"N
0°27'00.1"W

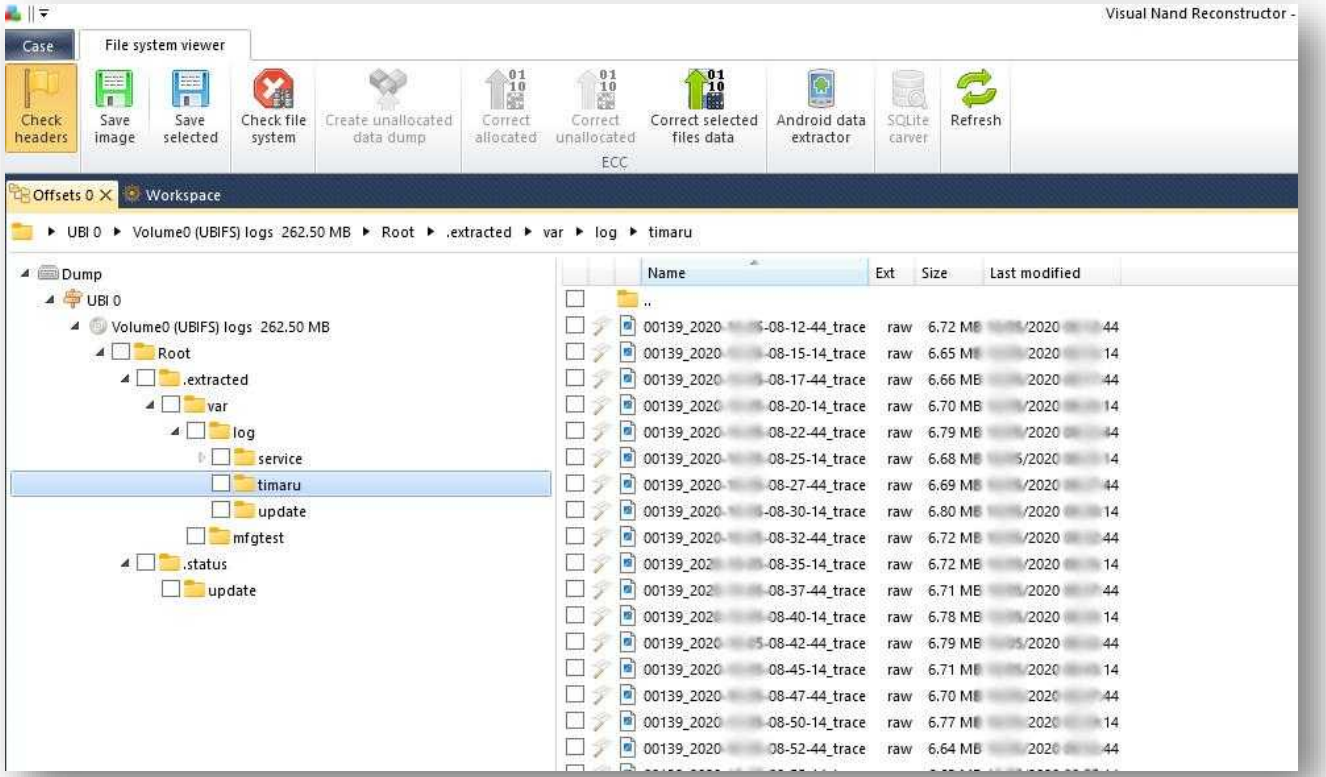
Isn't tractor a vehicle? ☺

ECU from auto-steering equipment of a tractor after fire accident. Analysed was conducted in order to establish the cause of an accident. Device was brought to analysis and system logs were extracted

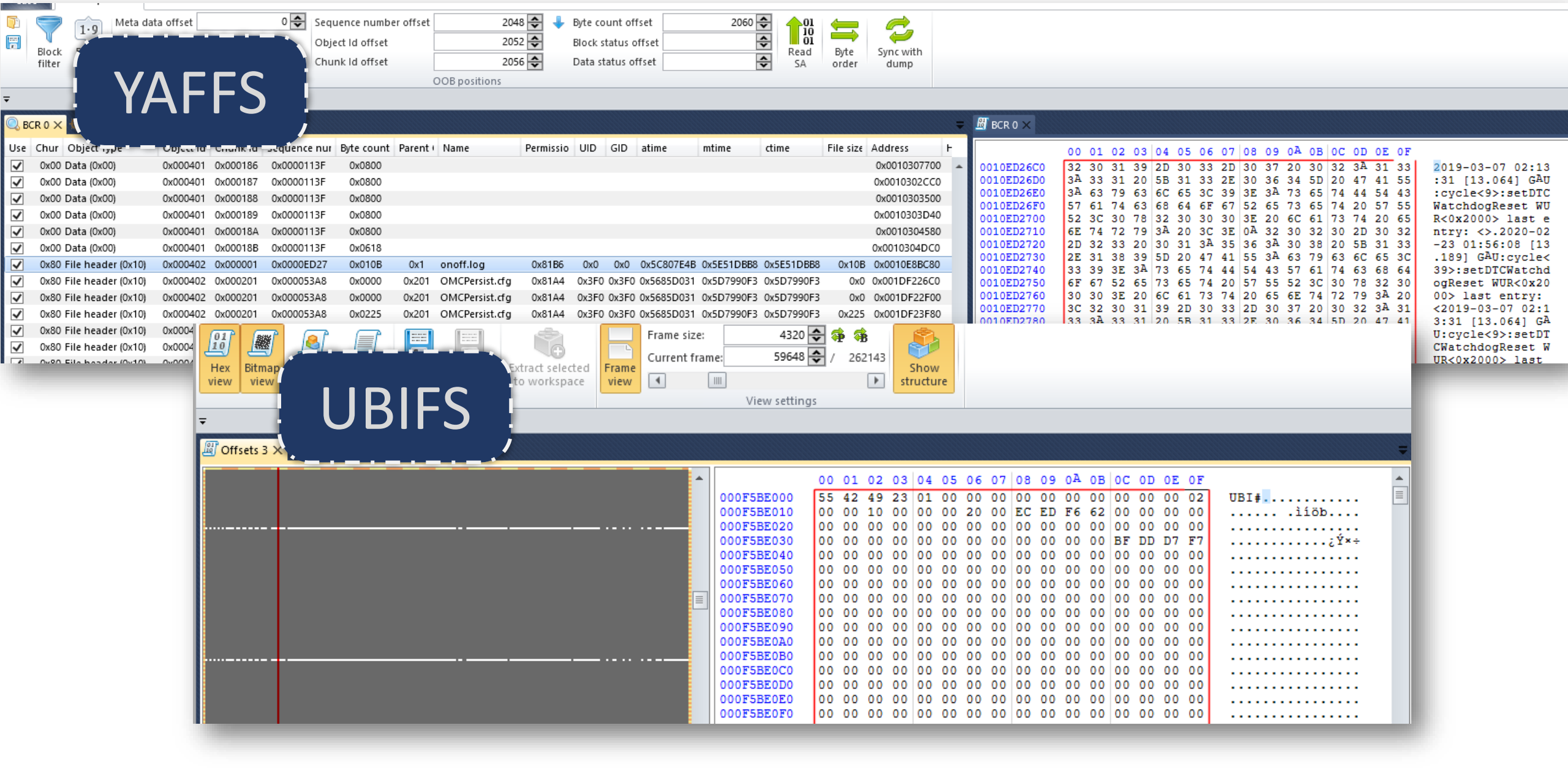


Physical image acquisition





Proprietary file systems in vehicles and IoT devices



Car stuff for research

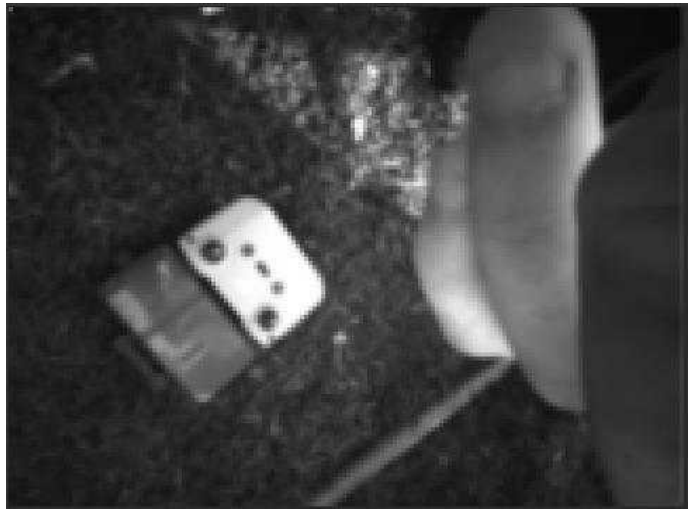
Over 160 car infotainment system checked so far!

BONUS – DJI Drones.
A new unique findings

Downward photograpths of the drone during launch





THANK YOU!!!

- Do you connect your phone to your rental car while on vacation?
- What is best method of data acquisition?
- Is it safe to start the car and boot system during investigation?
- Drones – what's better – GPS flight track or photos of launching site and drone's owner?

To learn more about this topic, join our conference on September 10-12 2024 in Warsaw, Poland

rusolut

www.rusolut.com
Polczynska 10,
Warsaw, Poland
+48 535 054 431
info@rusolut.com

Our partner

forsolution

www.forsolution.cz
Okružní 62, 250 84
Sibřina, Czech Republic
+420 608 361 321
info@forsolution.cz