

VEHICLE DIGITAL FORENSICS DATA ACQUISITION AND PROCESSING

Patryk Płudowski
Rusolut, Poland

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

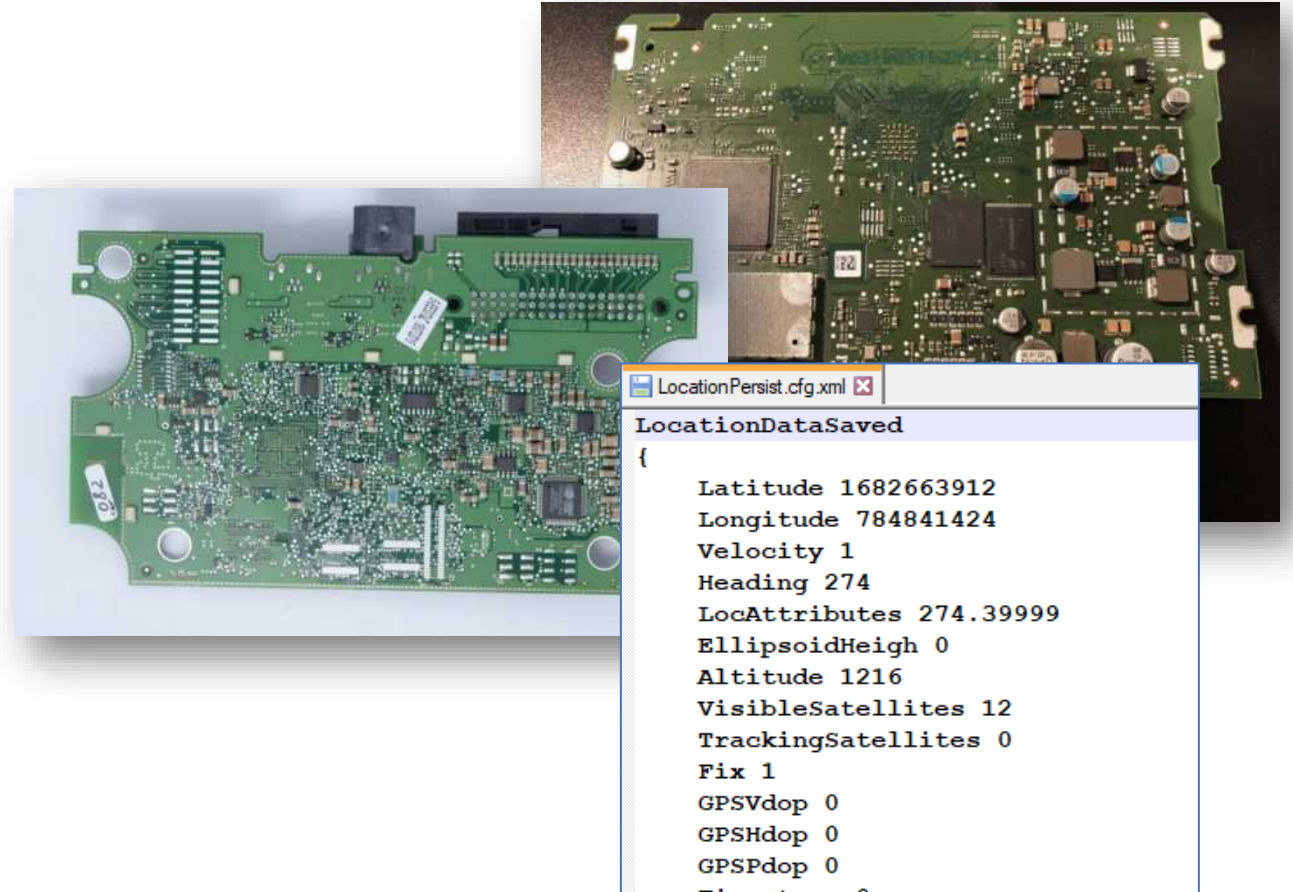
Every modern car has at least one data source, sometimes two or more.

Among others we have:

- Serial Number,
- VIN,
- fuel data,
- Power up and power down,
- Durations of trip,
- Radio usage...

If the system supports GPS:

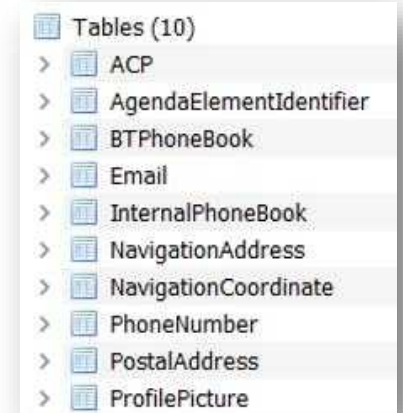
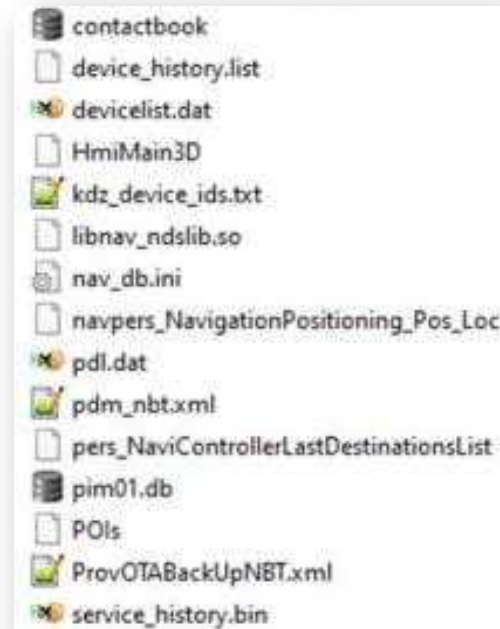
- destination,
- trips,
- Coordinates,
- Saved Locations...



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

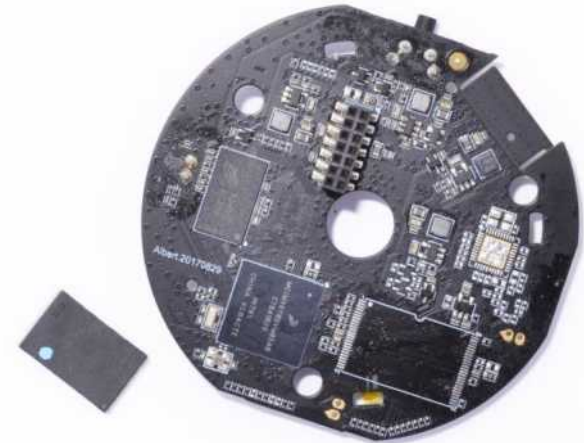
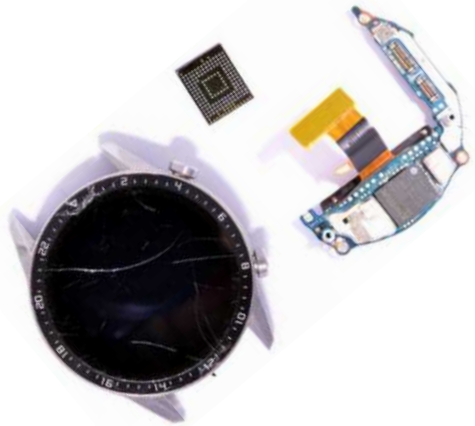


ApplicationTimeStamp.dat	19/12/2018 3:07 pm
Home.dat	21/03/2018 5:54 pm
LastDestination.db	19/12/2018 3:07 pm
LastRoute.dat	10/10/2018 2:55 am
POICategoryFilterMapView.dat	19/12/2018 3:04 pm
POICategoryFilterSearch.dat	18/05/2015 5:25 pm
PreferredAddress.db	18/05/2015 5:25 pm
Work.dat	15/09/2018 4:50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

Windows ► phonebook		
	Name	Ext
<input type="checkbox"/>	..	
<input type="checkbox"/>	CH2c5731cca418	xml
<input type="checkbox"/>	CH4cd1a12a1d05	xml
<input type="checkbox"/>	CH5848229af04e	xml
<input type="checkbox"/>	CH685acf211b7b	xml
<input type="checkbox"/>	CH6c4d7389d6f6	xml
<input type="checkbox"/>	GlobalPhonebook	txt
<input type="checkbox"/>	PB5848229af04e	SYN
<input type="checkbox"/>	PB685acf211b7b	SYN

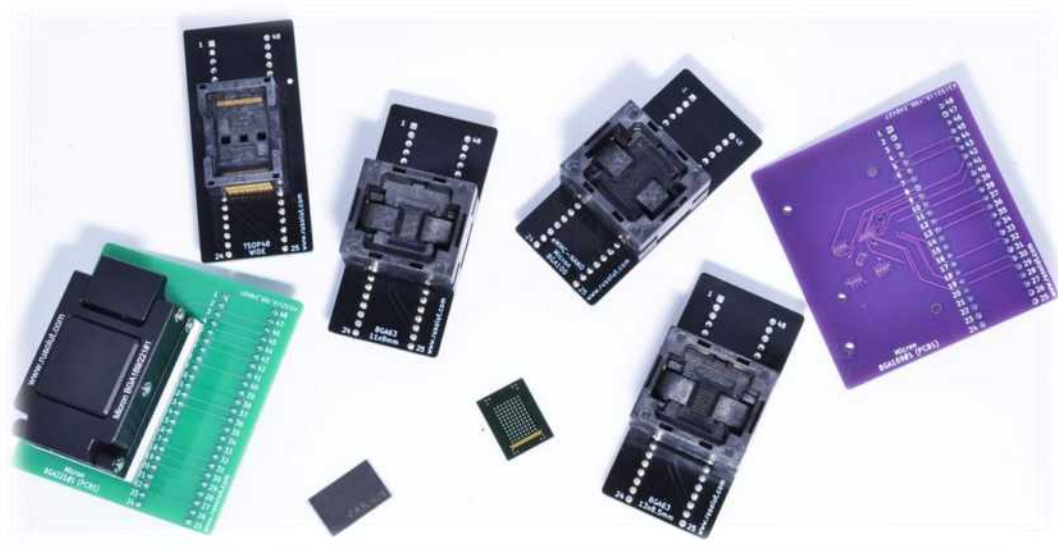
New Sources of Digital Evidence

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**.

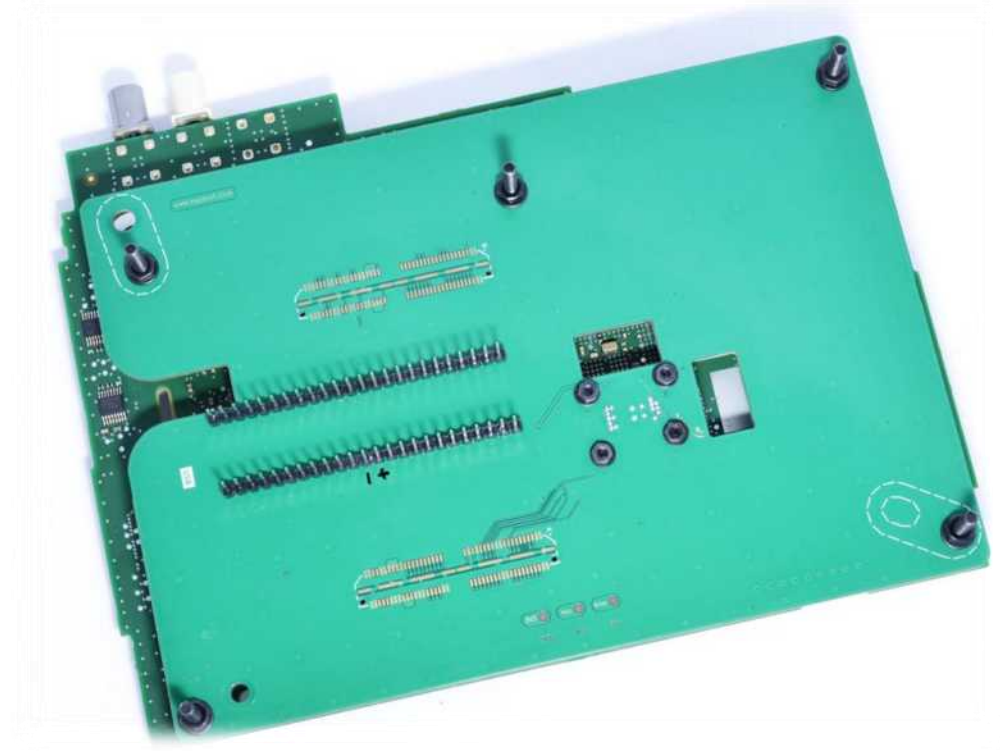


Direct methods of acquisition

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

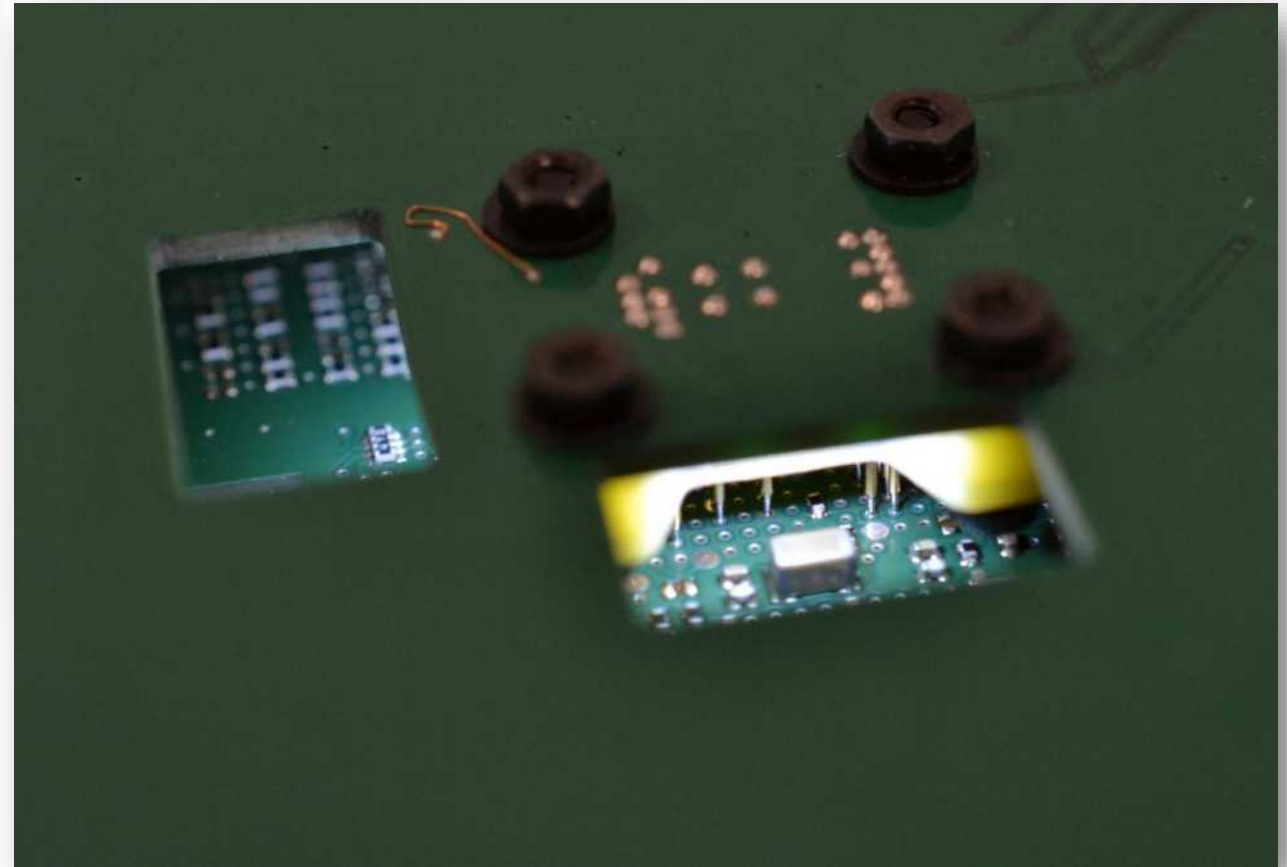
Chip-off

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

NEW Solderless adapters

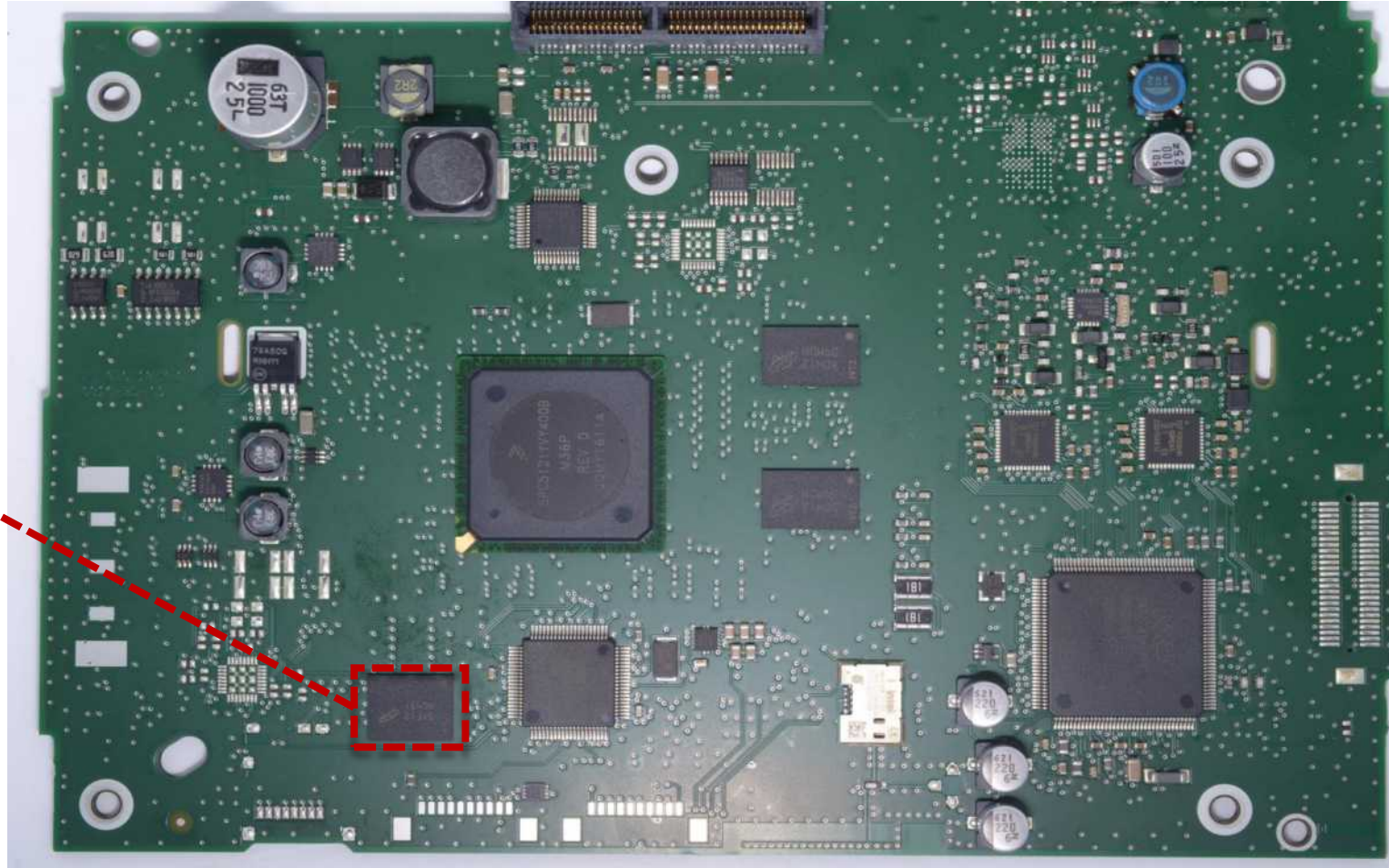
- Keeps PCB of system intact
- Much safer than regular chip-off

Solderless data acquisition

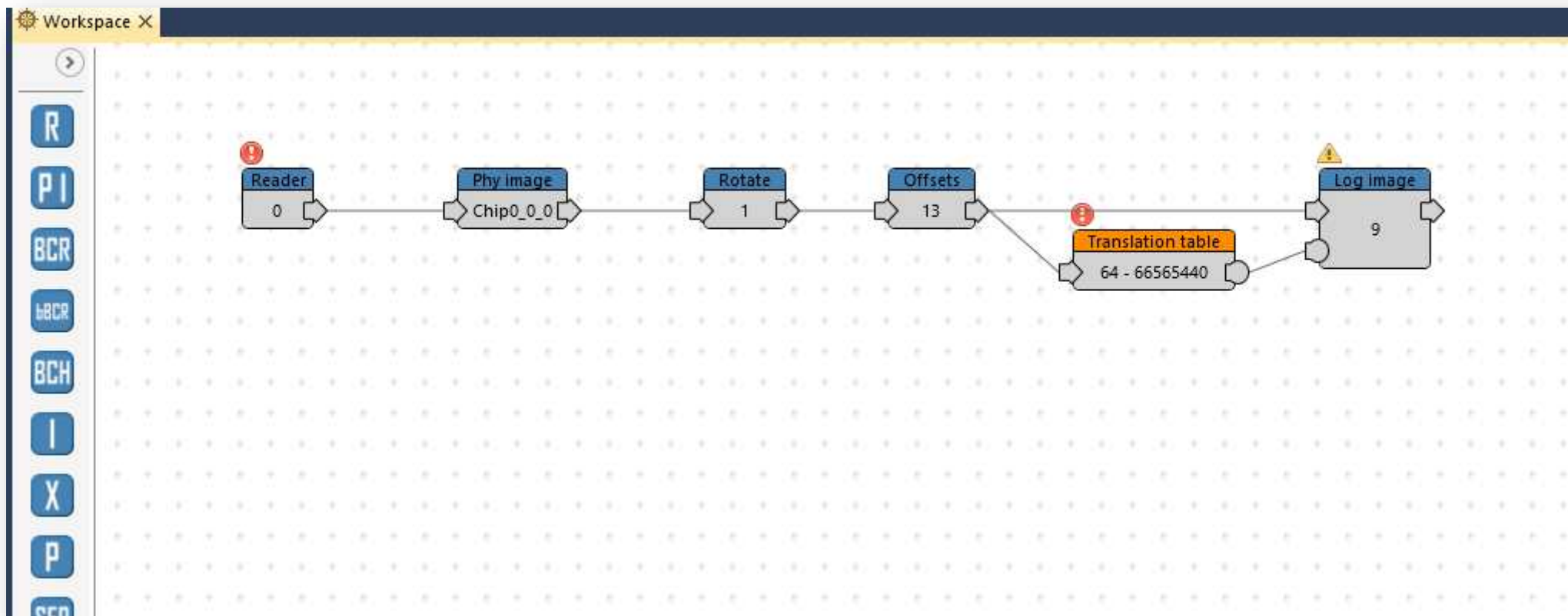


Peugeot 208 - real case scenario

NAND.
FLASH

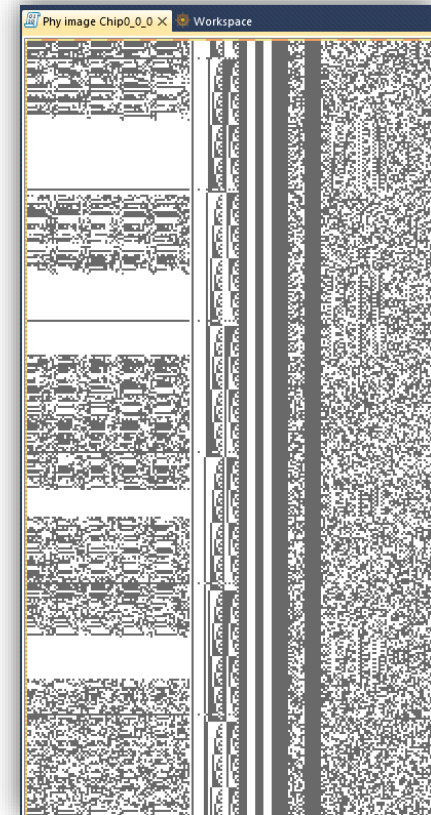
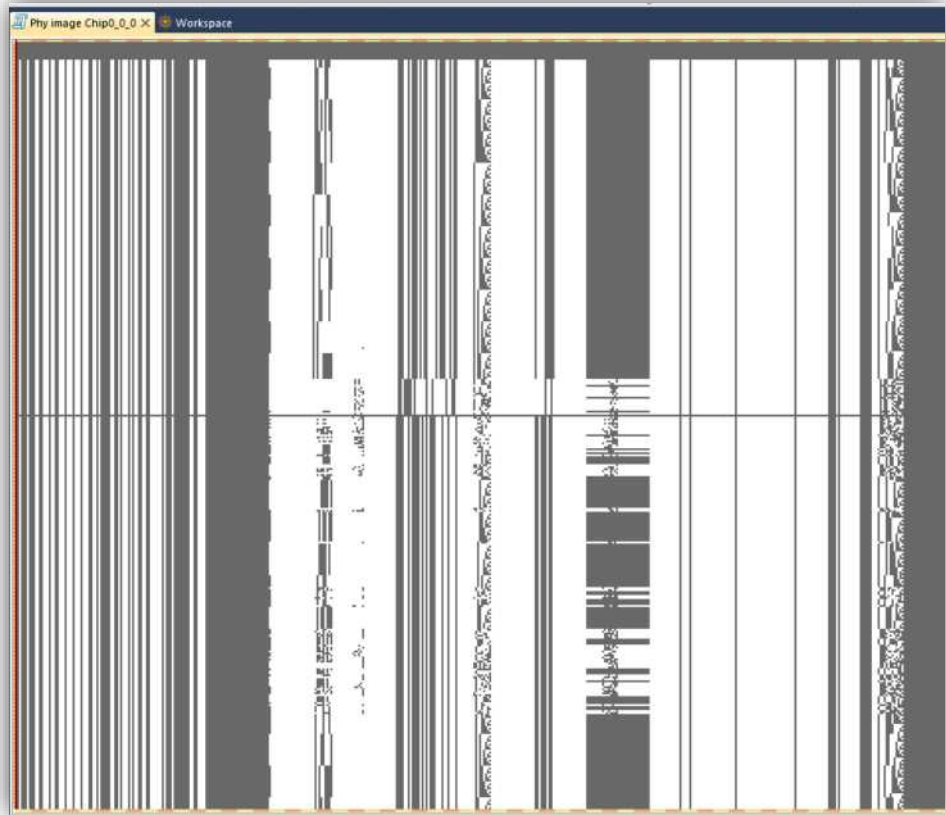


File structure reconstruction



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)

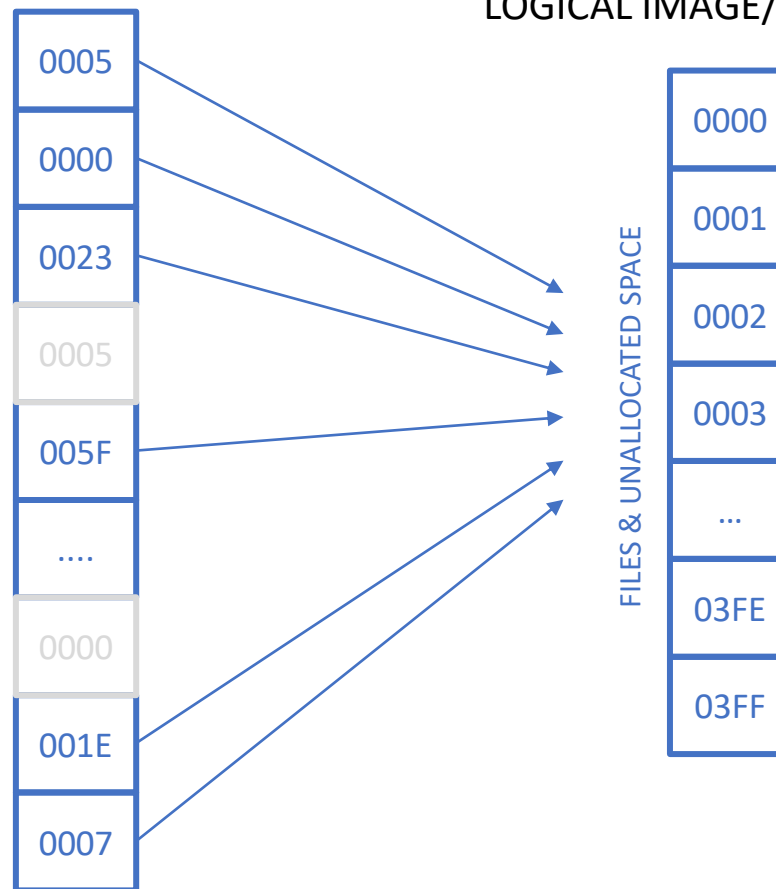


CONTROLLER WRITES DATA TO NAND MEMORY IN RANDOM ORDER
FLASH TRANSLATION LAYER IS USED TO STORE INFORMATION ABOUT THOSE PLACES

Translator - Block management

PHYSICAL IMAGE

LOGICAL IMAGE/FILE SYSTEMS



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

Logical Image Assembly

Translation table 64 - 66565440 X

Block (Static)						Page		
Use	Address	H	VID	BN	SN	Use	Address	LPN
<input checked="" type="checkbox"/>	470114304	1	66565440	0	29231	<input checked="" type="checkbox"/>	470116416	188
<input checked="" type="checkbox"/>	469708800	1	66565440	0	30288	<input checked="" type="checkbox"/>	470118528	189
<input checked="" type="checkbox"/>	469303296	1	66565440	0	31268	<input checked="" type="checkbox"/>	470120640	190
<input checked="" type="checkbox"/>	471060480	1	66565440	0	31269	<input checked="" type="checkbox"/>	470122752	191
<input checked="" type="checkbox"/>	470925312	1	66565440	0	31272	<input checked="" type="checkbox"/>	470124864	192
<input checked="" type="checkbox"/>	469843968	1	66565440	0	31277	<input checked="" type="checkbox"/>	470126976	195
<input checked="" type="checkbox"/>	470384640	1	66565440	0	31278	<input checked="" type="checkbox"/>	470129088	196
<input checked="" type="checkbox"/>	469573632	1	66565440	0	31279	<input checked="" type="checkbox"/>	470131200	198
<input checked="" type="checkbox"/>	471195648	1	66565440	0	31280	<input checked="" type="checkbox"/>	470133312	203
<input checked="" type="checkbox"/>	469168128	1	66565440	0	31281	<input checked="" type="checkbox"/>	470135424	204
<input checked="" type="checkbox"/>	469438464	1	66565440	0	31282	<input checked="" type="checkbox"/>	470137536	205
<input checked="" type="checkbox"/>	470654976	1	66565440	0	31283	<input checked="" type="checkbox"/>	470139648	206
<input checked="" type="checkbox"/>	470249472	1	66565440	0	31284	<input checked="" type="checkbox"/>	470141760	208
<input checked="" type="checkbox"/>	471330816	1	66565440	0	31285	<input checked="" type="checkbox"/>	470143872	210
<input checked="" type="checkbox"/>	470790144	1	66565440	0	31286	<input checked="" type="checkbox"/>	470145984	6
<input checked="" type="checkbox"/>	469979136	1	66565440	0	31287	<input checked="" type="checkbox"/>	470148096	7
<input checked="" type="checkbox"/>	470519808	1	66565440	0	31288	<input checked="" type="checkbox"/>	470150208	13
<input checked="" type="checkbox"/>	502149120	1	66565440	1	32	<input checked="" type="checkbox"/>	470152320	17
<input checked="" type="checkbox"/>	464707584	1	66565440	1	33	<input checked="" type="checkbox"/>	470154432	24

Log image 9 X Offsets 13 Workspace

Volume0 (Microsoft FAT16) 33.00 MB

Root

- address_book
- CRC
- internet_user
- user_data
- Audio
- sqlite
- T2BF
- TTS
- welcome_screen

FAT0

FAT1

!!!

Name	Ext	Size	Last modified
agenda	sqlite	123.00 KB	10/24/2018 07:55:34
config_options	sqlite	482 bytes	02/01/2000 00:01:04
config_options.sqlite	inf	48 bytes	02/01/2000 00:01:04
diagnosis	sqlite	1.06 KB	01/01/2007 00:10:50
diagnosis.sqlite	inf	48 bytes	01/01/2007 00:10:50
diag_zi	sqlite	2.57 KB	02/01/2000 00:00:58
diag_zi.sqlite	inf	49 bytes	02/01/2000 00:00:58
media_jkb_catalog	sqlite	557 bytes	02/01/2000 00:01:30
media_jkb_catalog.sqlite	inf	48 bytes	02/01/2000 00:01:30
Pictures	sqlite	1.24 KB	01/01/2007 00:10:52
Pictures.sqlite	inf	49 bytes	01/01/2007 00:10:52
Trip	sqlite	3.91 KB	01/01/2007 00:10:52
Trip.sqlite	inf	49 bytes	01/01/2007 00:10:52
up_common	sqlite	7.94 KB	01/01/2007 00:10:50
up_common.sqlite	inf	49 bytes	01/01/2007 00:10:50
up_config	sqlite	9.92 KB	01/19/2018 12:29:26
up_config.sqlite	inf	49 bytes	01/19/2018 12:29:26
up_user	sqlite	4.90 KB	01/01/2007 00:10:50
up_user.sqlite	inf	49 bytes	01/01/2007 00:10:50
up_user_hmi	sqlite	3.52 KB	01/01/2007 00:10:48
up_user_hmi.sqlite	inf	49 bytes	01/01/2007 00:10:48
version_history	sqlite	238 bytes	02/01/2000 00:01:30
version_history.sqlite	inf	48 bytes	02/01/2000 00:01:30

IN VNR WE CAN CREATE MODEL WITH ADVANCED TRANSLATORS

Overview of data that can be extracted

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

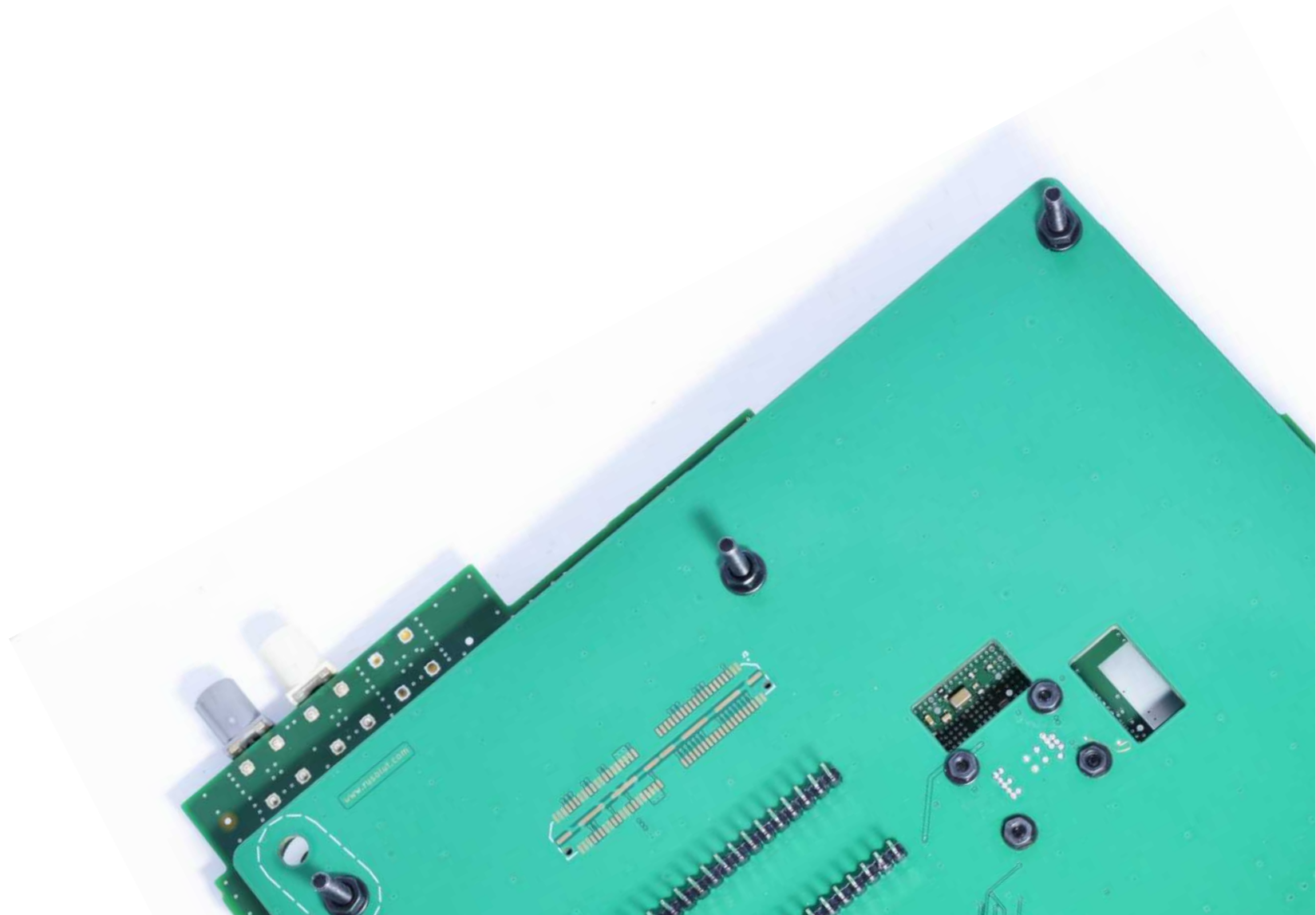
Total: 117

```

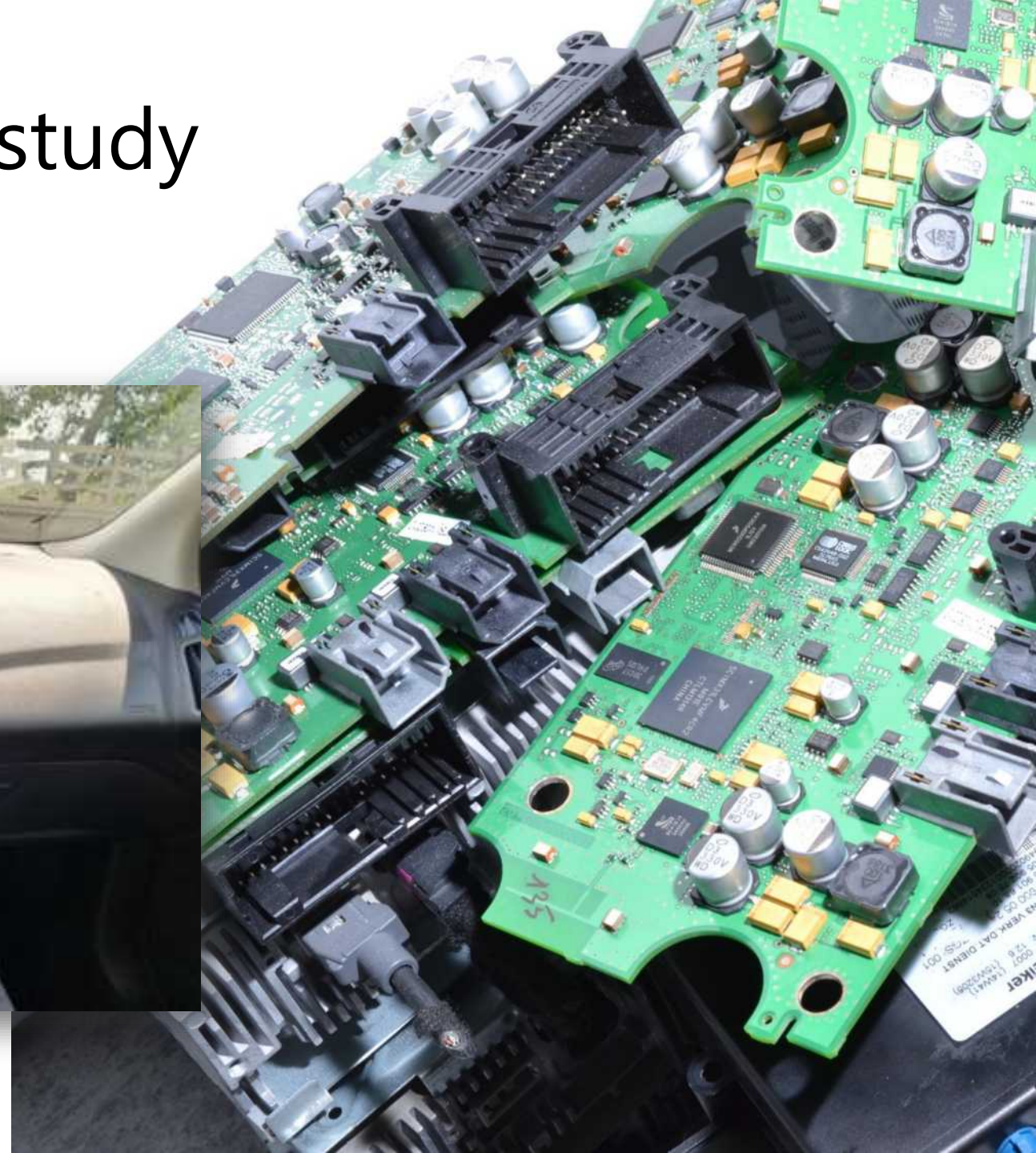
K.....Peugeot.....
.....|.....
.....
.....žėÇ.ž,×.žėÇ..ėÇ.žėÇ.....ž
=M=p8Ė10+50[iXØT2.L.ŽŪ."=Sjh.0%%.uákT..zñ^Ū.Ū
"@'ŌĀĖŠē?à...9..Ė.'$P'i~¥$Ū±~äûZŪĭĀM...S.¤÷<ĖX'7
.i"¤¤÷<ñ(ĀĖ7(w2)fðN".p%.....
Samsung Galaxy S7 edge.....
VFD 600.....
MID4010.....
Galaxy A3 (2016).....
Samsung Galaxy S7 edge.....
Galaxy Note8.....
GT-I8260.....
Galaxy A5 (2017).....
.....
.....
-[.....
.....

```

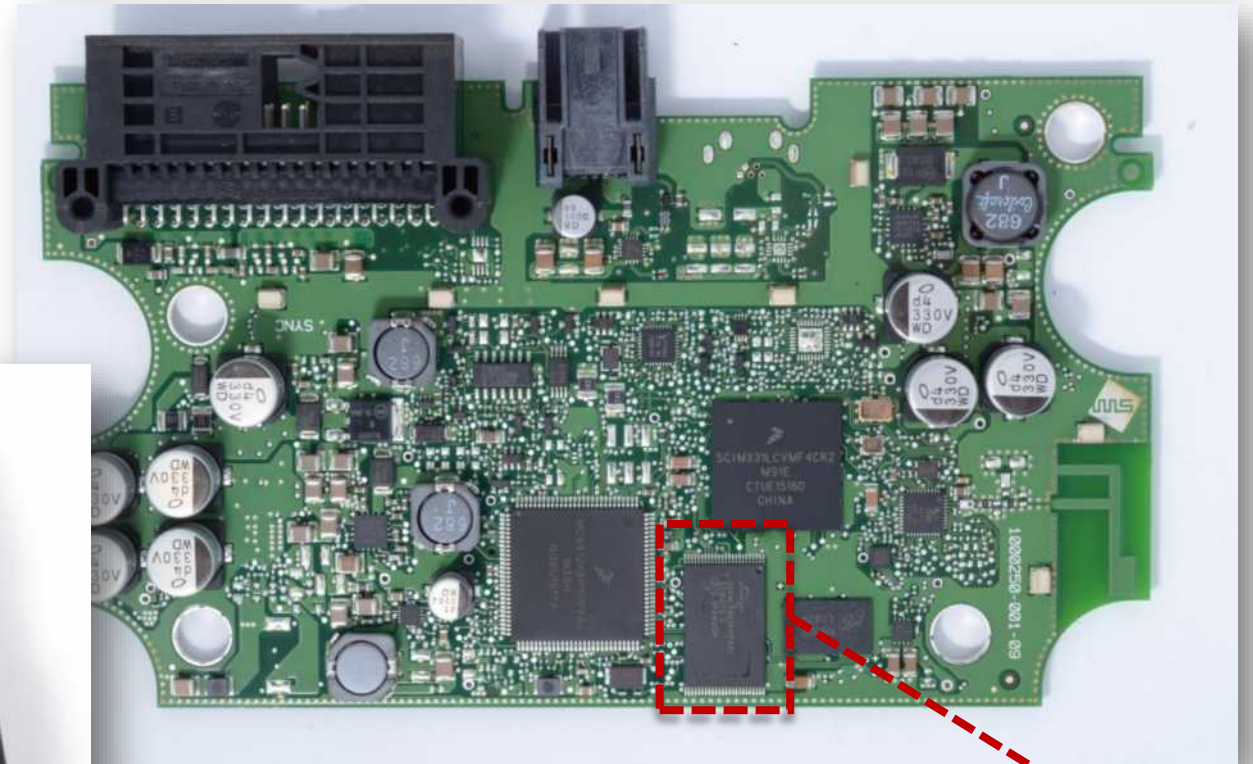
Hands on case study – live demo



Ford Sync – case study



Ford Sync – user data overview



NAND
FLASH

List of connected devices

```
9805 >>>> Paired devices(0x00000007):
9807     device: 3. [David's iPhone] [0x0000c88507a312], active = 0, primary = 1,
9818     device: 5. [Bawbags ipod] [0x0000d8d1c257d0], active = 0, primary = 0, pa
9829     device: 4. [JULES JUKE BOX] [0x00002cf4e3627d], active = 0, primary = 0,
9840     device: 2. [D2303] [0x000044d4e0ba5071], active = 0, primary = 0, pairorder
9850     device: 1. [BAWBAG] [0x0000bccfccefb4c], active = 0, primary = 0, pairorde
```

```
1669825 MPCoreDump: Index #0, Device id [name:JULES JUKE BOX][serial:CCQN][protocol:6
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:DNQL][protocol:6
1669856 MPCoreDump: Type = Persisted. , Src Id 1, Port 1, State 0x11
1669862 MPCoreDump: DeviceId: [name:David's iPhone][serial:DNQL][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 d8d1c257d0.
1669890 MPCoreDump: Type = Persisted. , Src Id 3, Port 3, State 0x11
1669896 MPCoreDump: DeviceId: d8d1c257d0.
1669900 MPCoreDump: Index #4, Device id [name:David's iPhone][serial:F17F][protocol:6
1669909 MPCoreDump: Type = Persisted. , Src Id 4, Port 1, State 0x11
1669915 MPCoreDump: DeviceId: [name:David's iPhone][serial:F17F][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:2.22.20
```

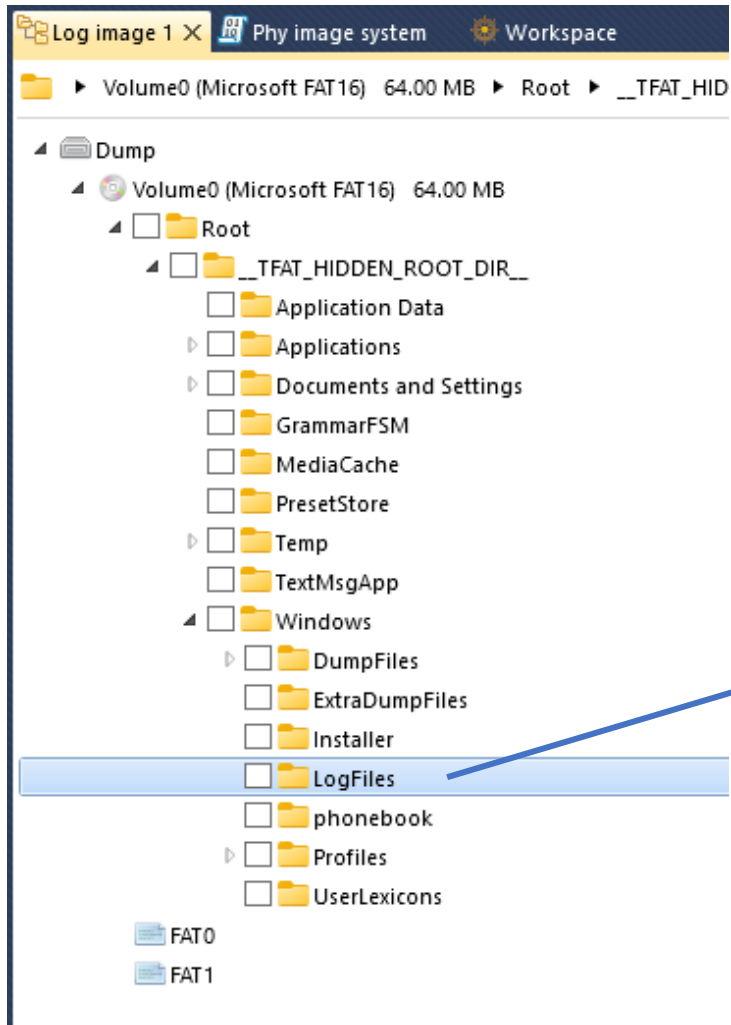
Call log and phone book

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 bry 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 ne =
22	43	68	65	6C	22	20	6E	75	6D	3D	22	30	37	34	32	"Che num="0 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=" 7010000 "
2F	3E	0D	0A	09	09	3C	43	61	6C	6C	20	6E	61	6D	65	/>.. <Call ne
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 >....<0 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 >....<0 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... hÄÿ... ..
09	00	D0	96	D0	B0	D0	BD	D0	B0	00	01	00	01	00	0F	..B "B%B".....
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	00Zak.....
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	350773683255
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	390746642309
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	120Vasil^
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	004Vasil
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	nsi074920
36	37	37	35	38	00	1A	00	00	00	06	00	56	61	6C	69	677Vali
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	191Toncat
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	310Tommy
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

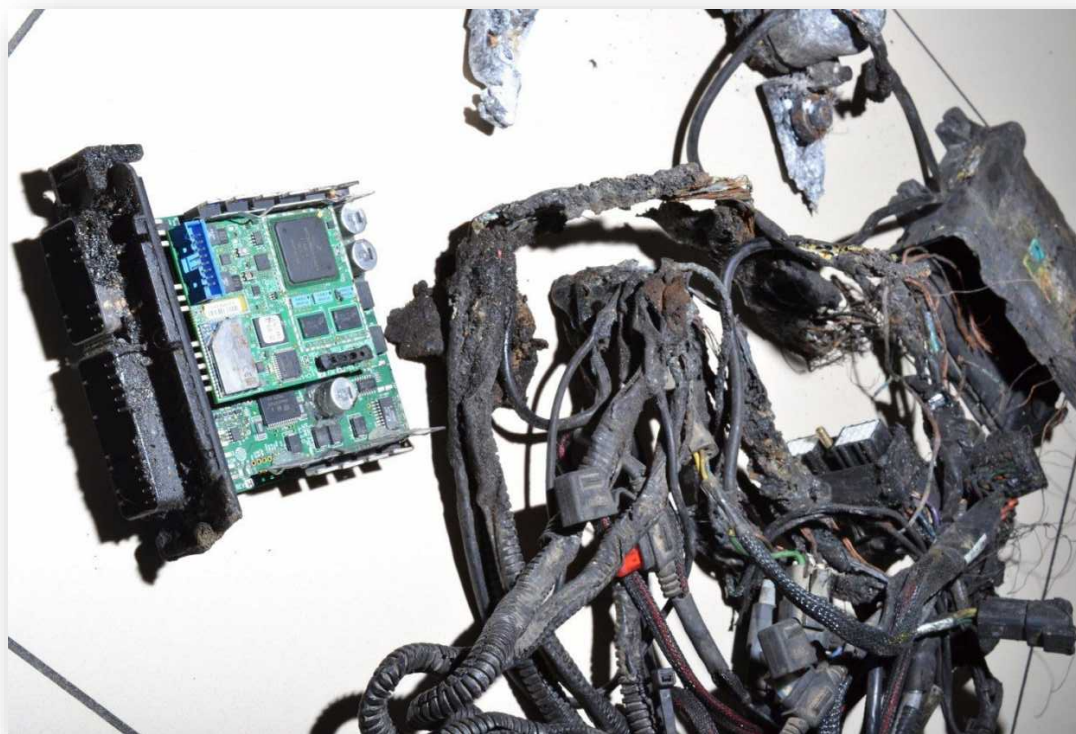


51°49'51.9"N
0°27'00.1"W



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



YAFFS



Car stuff for research

Over 160 car
infotainment system
checked so far!



BONUS – DJI Drones. A new unique findings



Downward camera sensor of Visual Positioning System (VSP)



Downward photographs 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?



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

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

Our partner



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