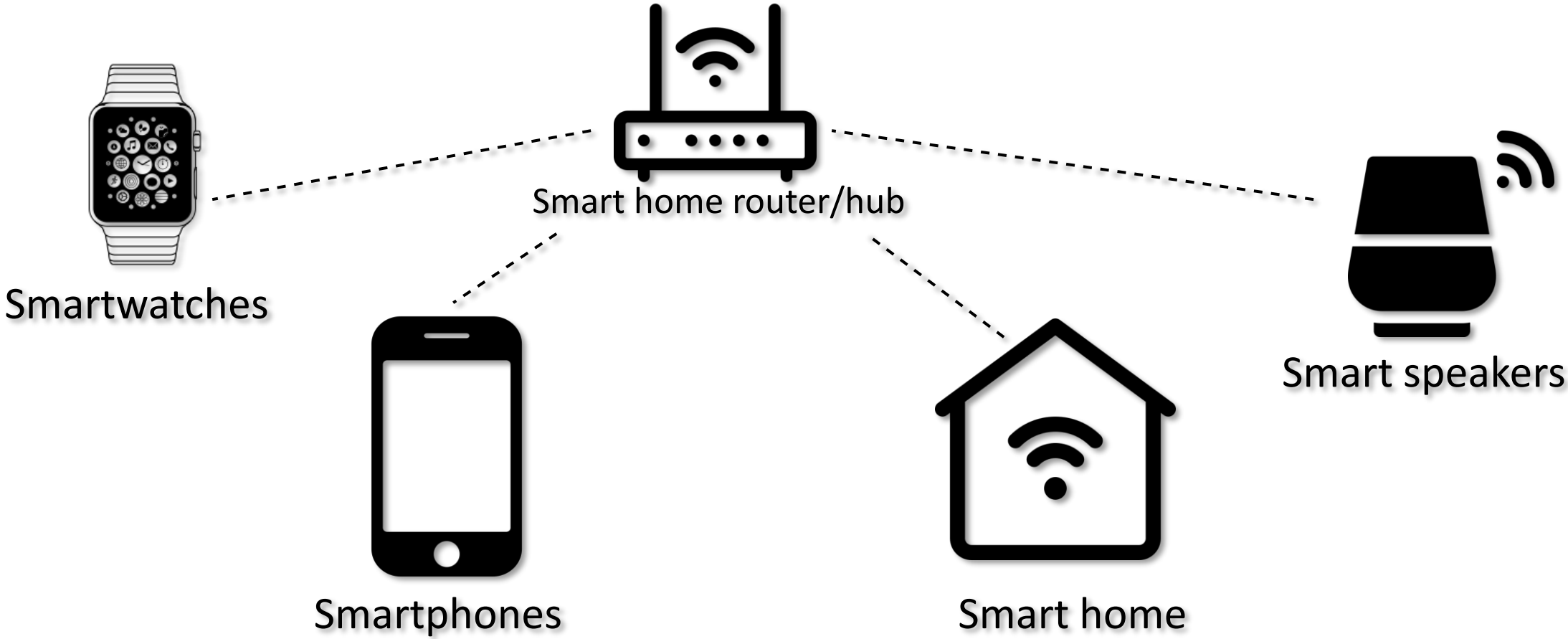
Ekstrakcja dowodów z urządzeń IoT z wykorzystaniem metody Chip-off

Michał Gmurek – Rusolut, Poland

PTXXI 2022 IV Konferencja Naukowa
PRZESTĘPCZOŚĆ TELEINFORMATYCZNA XXI WIEKU

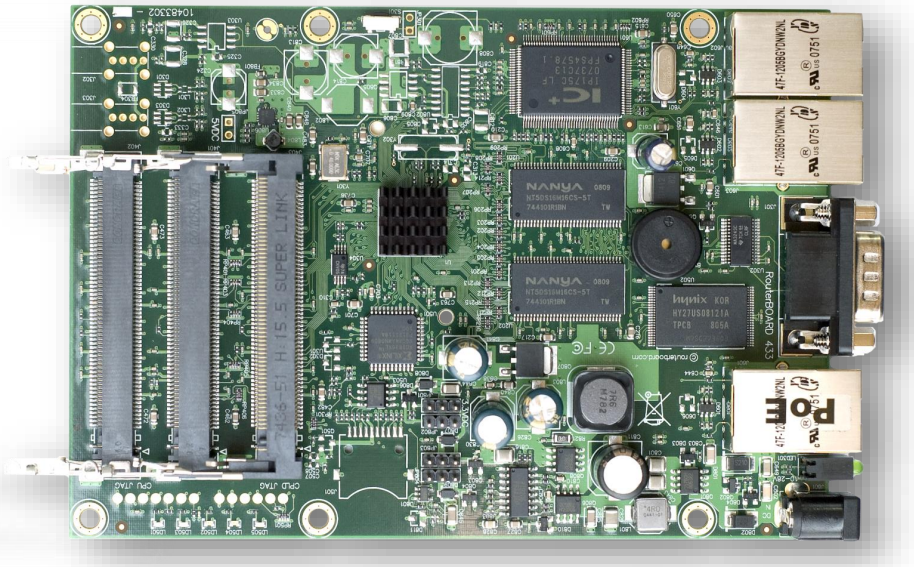
Urządzenia IoT



Badane urządzenia

CALIX 844E-1

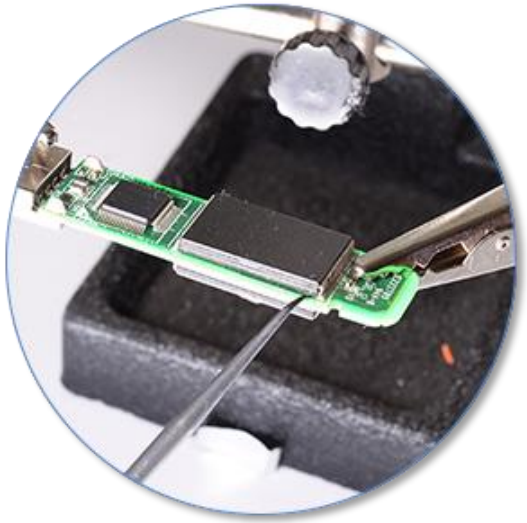
Mikrotik RB433GL



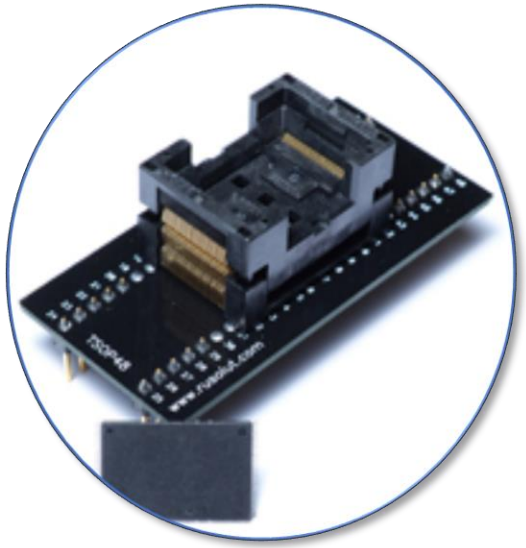
Google Home Speaker

Odzyskiwanie danych metodą Chip-off

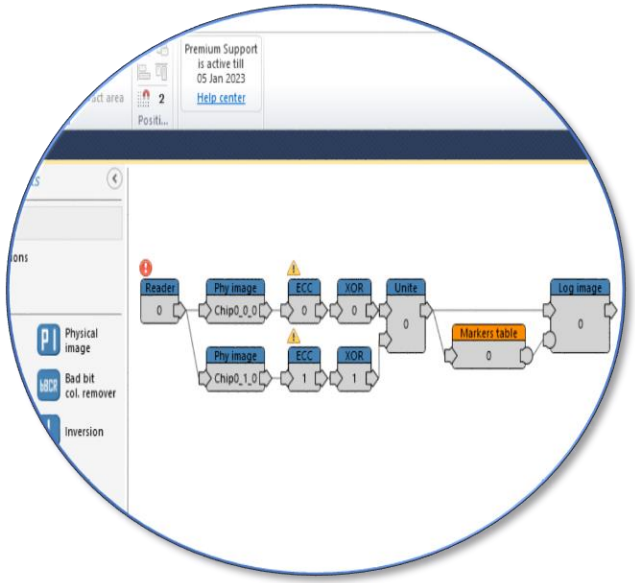
Wylutowanie kości pamięci NAND



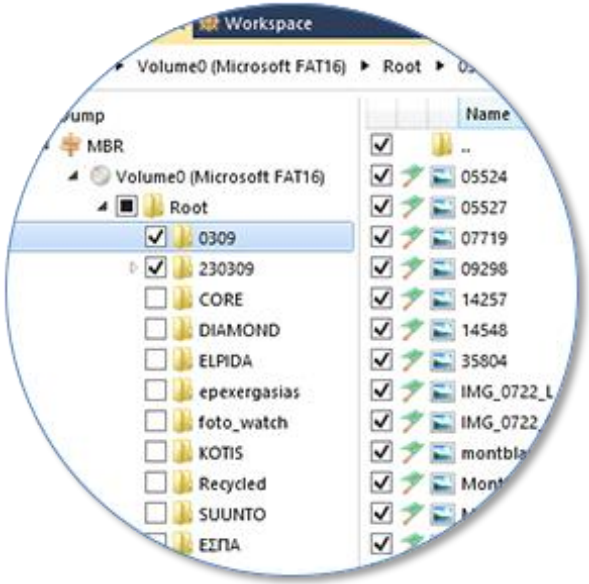
Identyfikacja chipu oraz dobór adaptera



Wyczytanie pamięci i rekonstrukcja obrazu fizycznego



Analiza obrazu logicznego oraz zapisanie danych



Zalety odzyskiwania danych metodą Chip-off

- Brak ryzyka nadpisania danych oraz logów urządzenia
- Dostęp do danych urządzeń chronionych hasłem
- Dostęp do wszystkich danych zgromadzonych na urządzeniu
- Możliwość odzyskania danych z uszkodzonych urządzeń
- Dostęp do danych usuniętych przez standardowy interfejs

Wbudowane systemy plików flash urządzeń IoT
YAFFS, UBI FS, NAND FS, RAW

Funkcje

- Optymalizacja zużycia bloków pamięci NAND (Wear leveling)
- Translacja fizycznego obrazu do postaci logicznej
- Operacje odświeżania danych zapisanych w blokach pamięci NAND

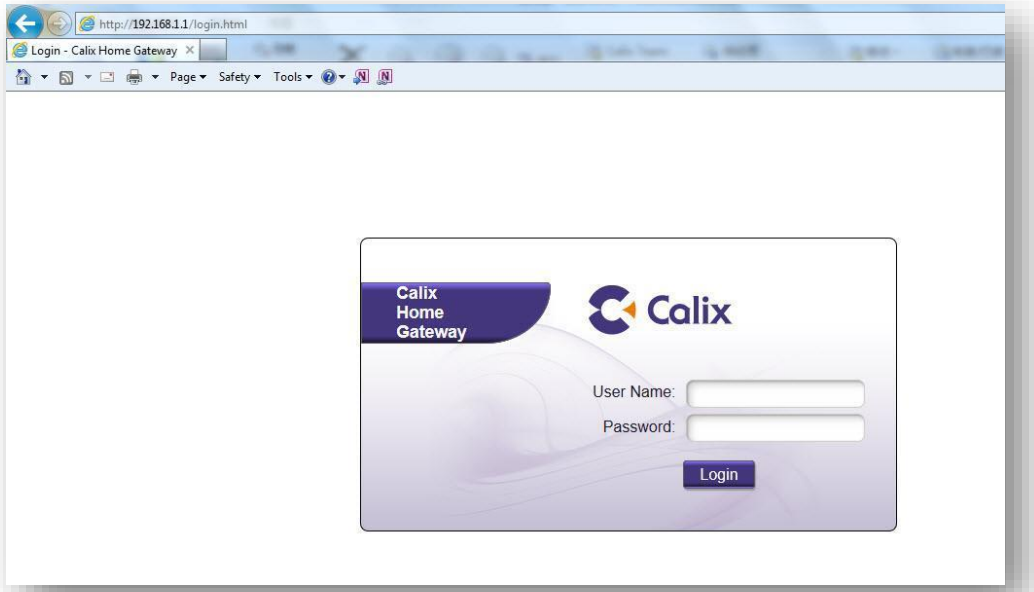
Właściwości

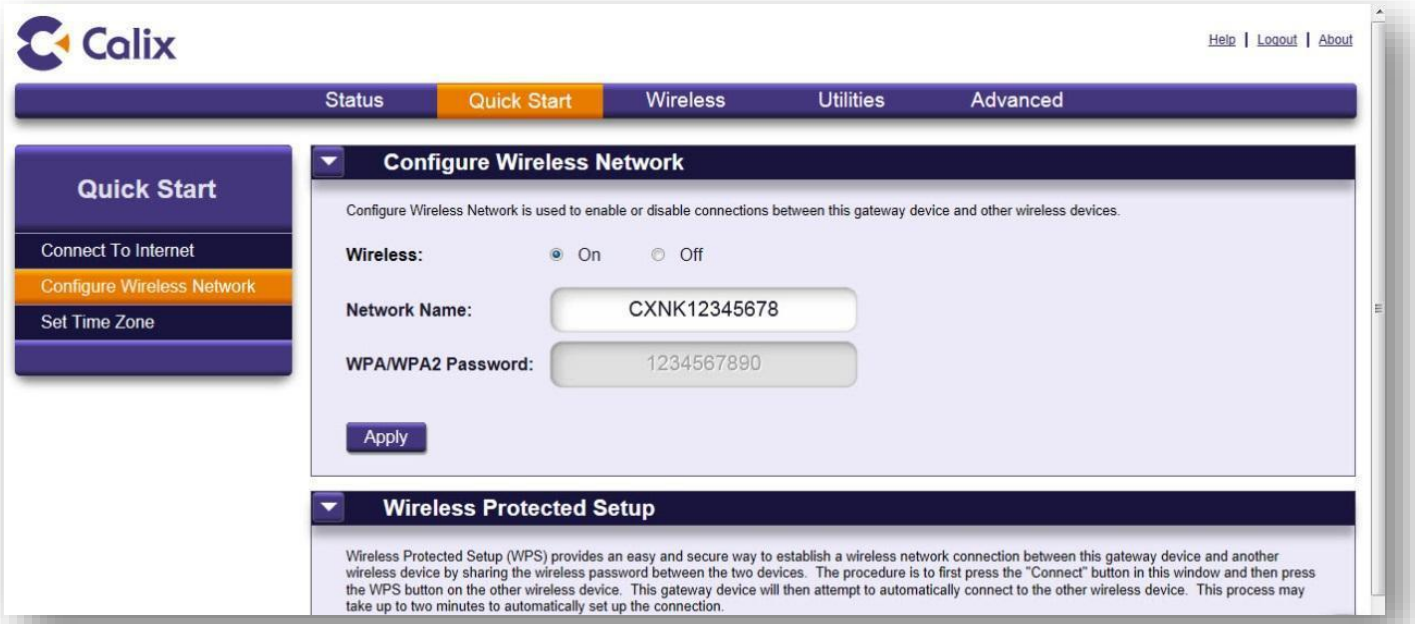
- Wiele wersji systemów pliku
- Brak ustandaryzowanych metadanych
- Możliwości odzyskiwania starych/skasowanych danych

Case 1 - CALIX 844E-1

CALIX 844E-1

Oprogramowanie sieciowe



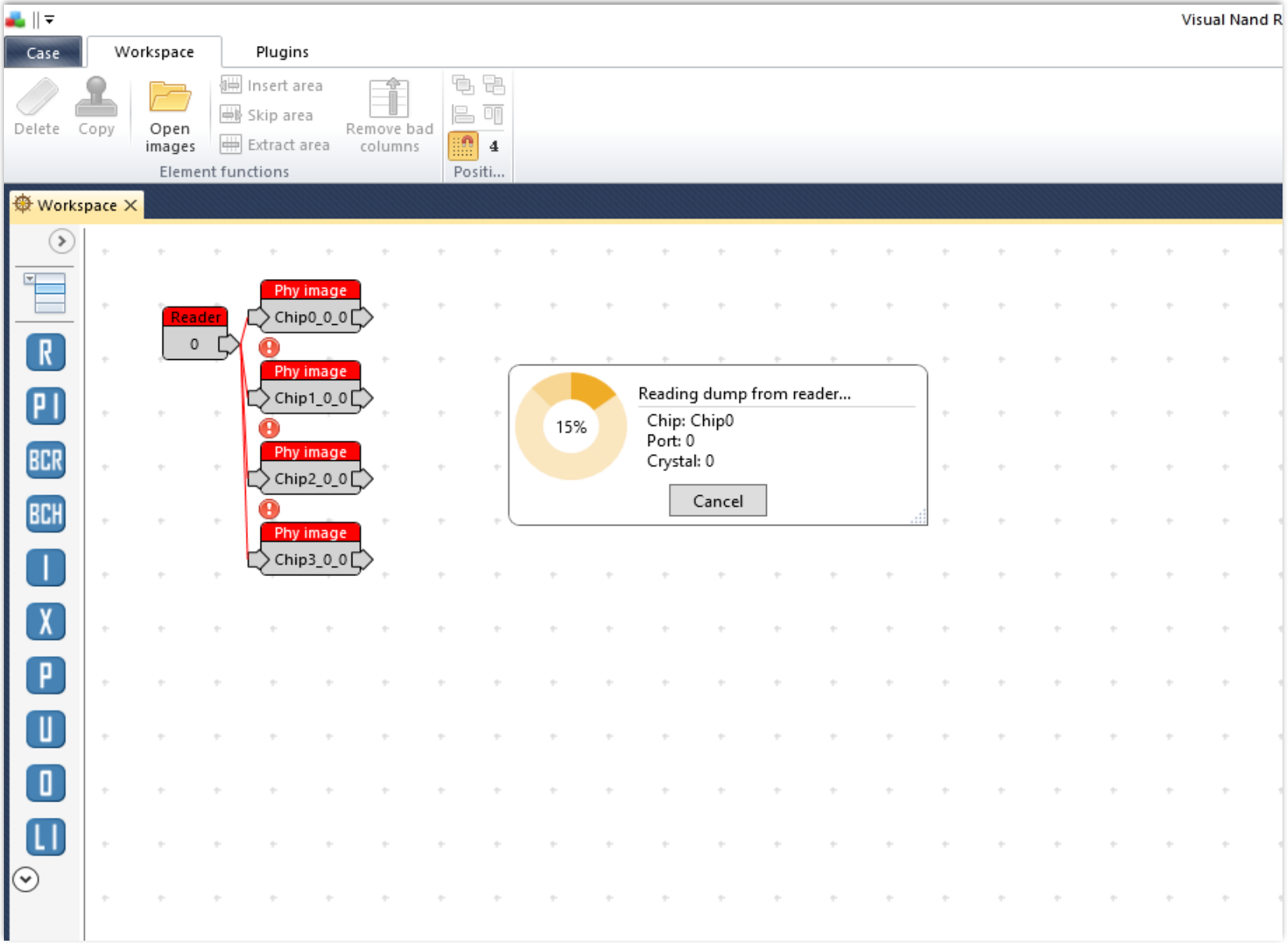


CALIX 844E-1

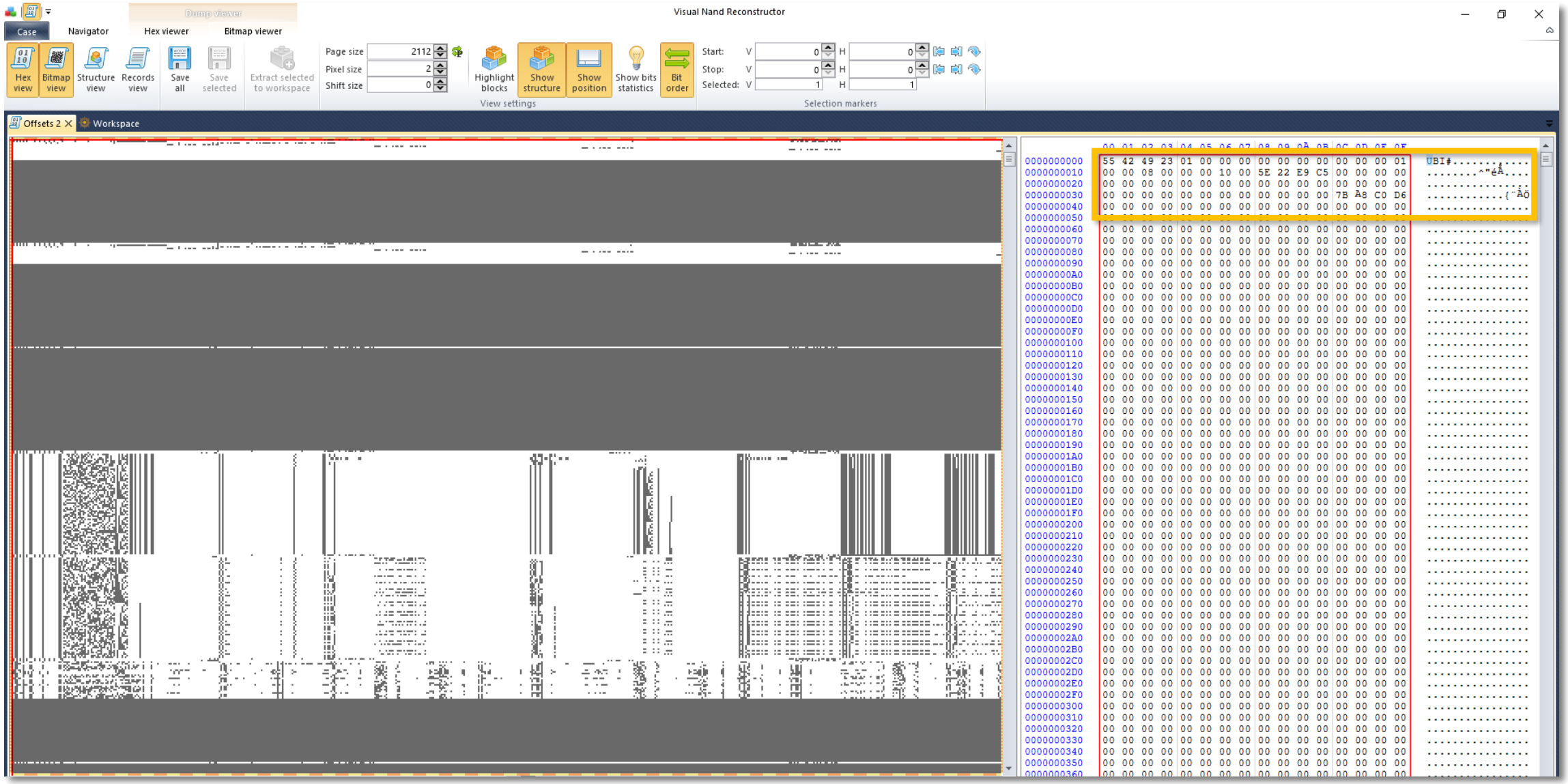
PCB

Odczyt zawartości kości pamięci w VNR

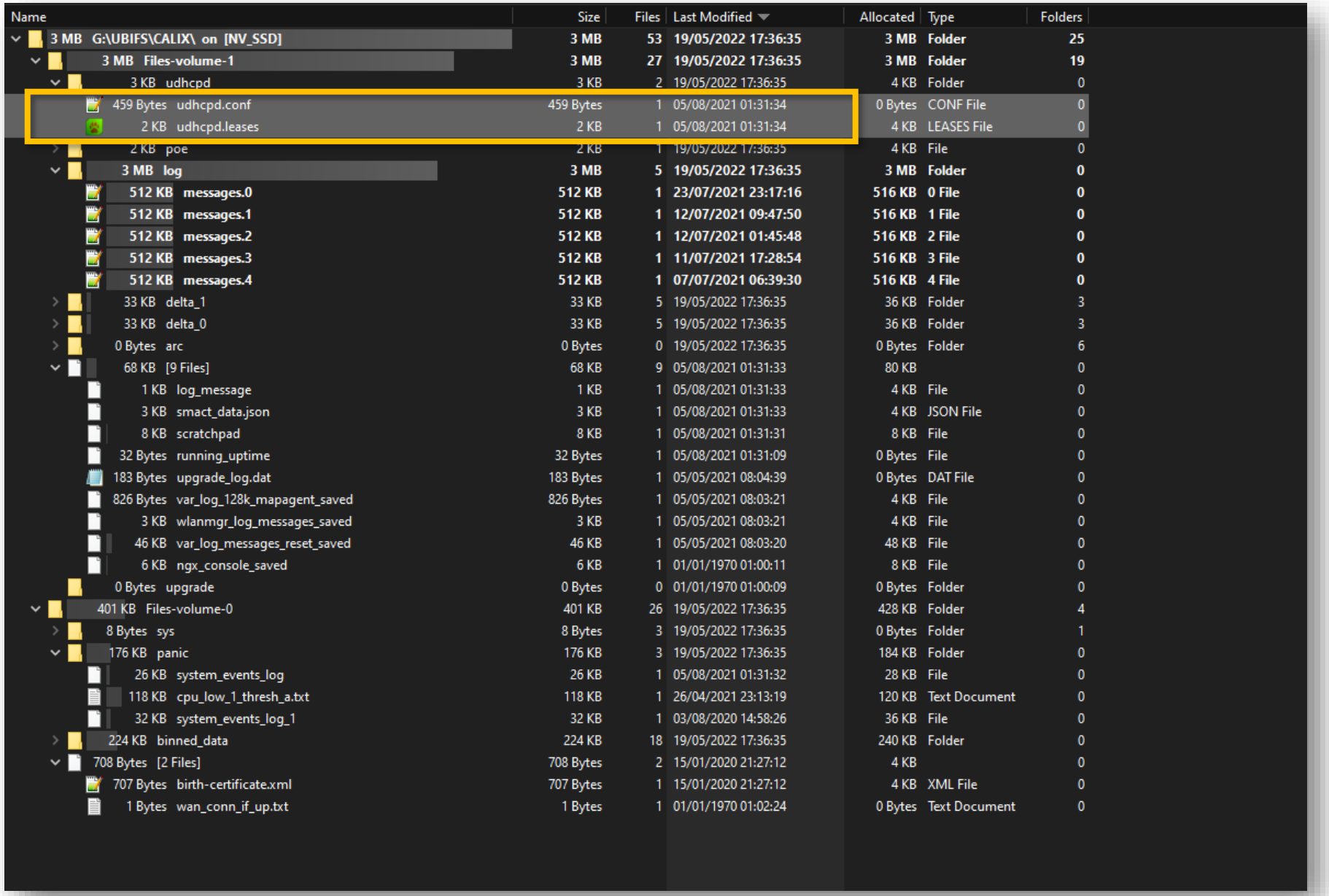
Proces czytania pamięci NAND



Wyczytany obraz fizyczny

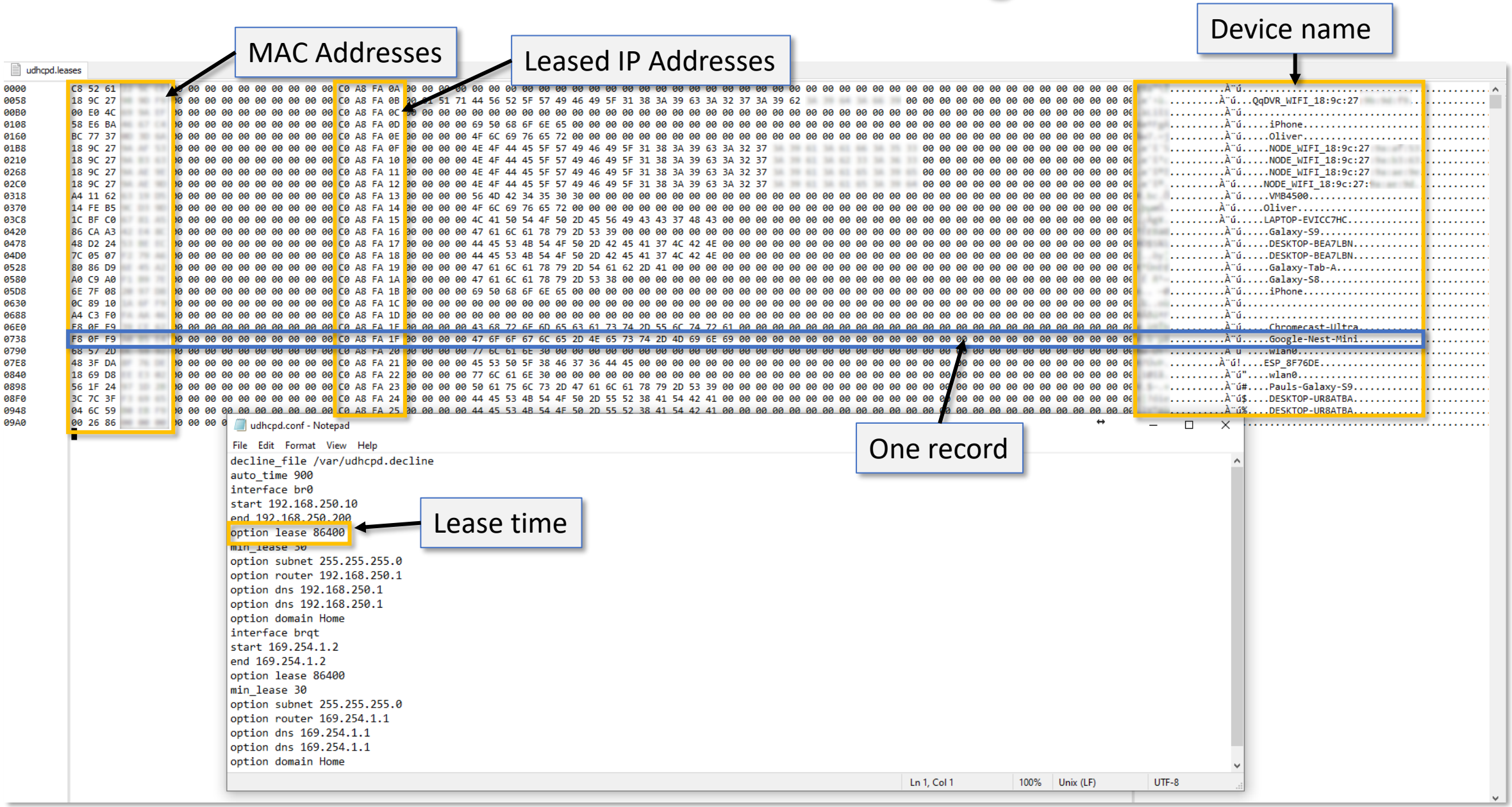


UBI File System



Name	Size	Files	Last Modified	Allocated	Type	Folders
3 MB G:\UBIFS\CALIX\ on [NV_SSD]	3 MB	53	19/05/2022 17:36:35	3 MB	Folder	25
3 MB Files-volume-1	3 MB	27	19/05/2022 17:36:35	3 MB	Folder	19
3 KB udhcpd	3 KB	2	19/05/2022 17:36:35	4 KB	Folder	0
459 Bytes udhcpd.conf	459 Bytes	1	05/08/2021 01:31:34	0 Bytes	CONF File	0
2 KB udhcpd.leases	2 KB	1	05/08/2021 01:31:34	4 KB	LEASES File	0
2 KB poe	2 KB	1	19/05/2022 17:36:35	4 KB	File	0
3 MB log	3 MB	5	19/05/2022 17:36:35	3 MB	Folder	0
512 KB messages.0	512 KB	1	23/07/2021 23:17:16	516 KB	0 File	0
512 KB messages.1	512 KB	1	12/07/2021 09:47:50	516 KB	1 File	0
512 KB messages.2	512 KB	1	12/07/2021 01:45:48	516 KB	2 File	0
512 KB messages.3	512 KB	1	11/07/2021 17:28:54	516 KB	3 File	0
512 KB messages.4	512 KB	1	07/07/2021 06:39:30	516 KB	4 File	0
33 KB delta_1	33 KB	5	19/05/2022 17:36:35	36 KB	Folder	3
33 KB delta_0	33 KB	5	19/05/2022 17:36:35	36 KB	Folder	3
0 Bytes arc	0 Bytes	0	19/05/2022 17:36:35	0 Bytes	Folder	6
68 KB [9 Files]	68 KB	9	05/08/2021 01:31:33	80 KB		0
1 KB log_message	1 KB	1	05/08/2021 01:31:33	4 KB	File	0
3 KB smact_data.json	3 KB	1	05/08/2021 01:31:33	4 KB	JSON File	0
8 KB scratchpad	8 KB	1	05/08/2021 01:31:31	8 KB	File	0
32 Bytes running_uptime	32 Bytes	1	05/08/2021 01:31:09	0 Bytes	File	0
183 Bytes upgrade_log.dat	183 Bytes	1	05/05/2021 08:04:39	0 Bytes	DAT File	0
826 Bytes var_log_128k_mapagent_saved	826 Bytes	1	05/05/2021 08:03:21	4 KB	File	0
3 KB wlanmgr_log_messages_saved	3 KB	1	05/05/2021 08:03:21	4 KB	File	0
46 KB var_log_messages_reset_saved	46 KB	1	05/05/2021 08:03:20	48 KB	File	0
6 KB ngx_console_saved	6 KB	1	01/01/1970 01:00:11	8 KB	File	0
0 Bytes upgrade	0 Bytes	0	01/01/1970 01:00:09	0 Bytes	Folder	0
401 KB Files-volume-0	401 KB	26	19/05/2022 17:36:35	428 KB	Folder	4
8 Bytes sys	8 Bytes	3	19/05/2022 17:36:35	0 Bytes	Folder	1
176 KB panic	176 KB	3	19/05/2022 17:36:35	184 KB	Folder	0
26 KB system_events_log	26 KB	1	05/08/2021 01:31:32	28 KB	File	0
118 KB cpu_low_1_thresh_a.txt	118 KB	1	26/04/2021 23:13:19	120 KB	Text Document	0
32 KB system_events_log_1	32 KB	1	03/08/2020 14:58:26	36 KB	File	0
224 KB binned_data	224 KB	18	19/05/2022 17:36:35	240 KB	Folder	0
708 Bytes [2 Files]	708 Bytes	2	15/01/2020 21:27:12	4 KB		0
707 Bytes birth-certificate.xml	707 Bytes	1	15/01/2020 21:27:12	4 KB	XML File	0
1 Bytes wan_conn_if_up.txt	1 Bytes	1	01/01/1970 01:02:24	0 Bytes	Text Document	0

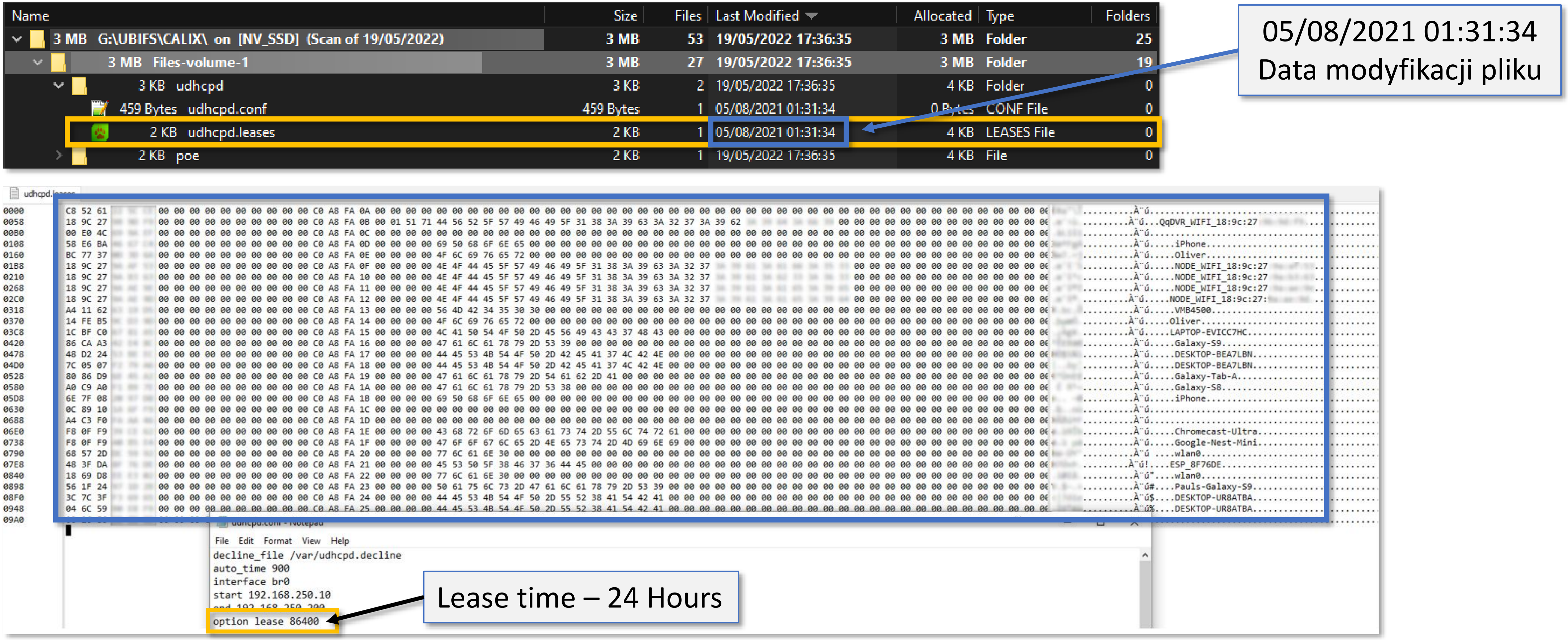
DHCP Leases i Config



ruSolut

Case 1 - Podsumowanie

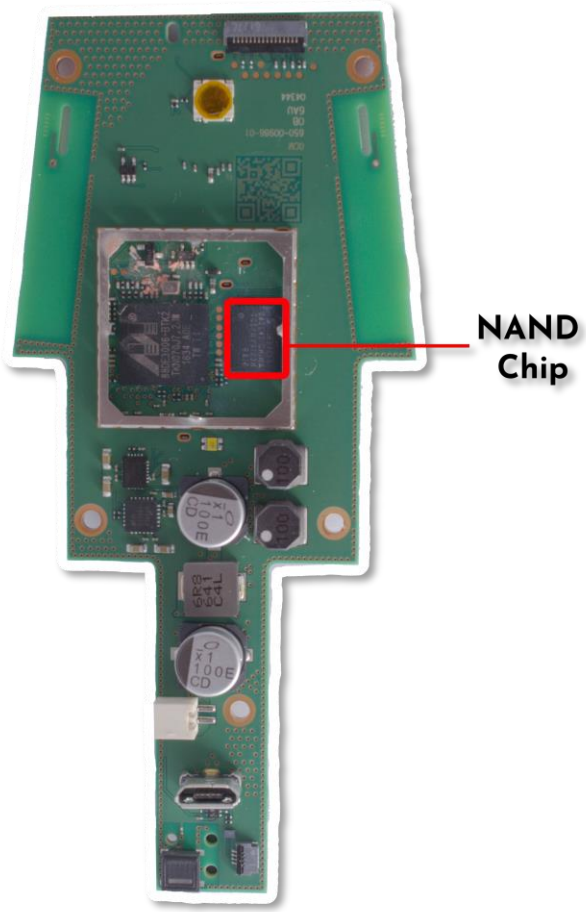
Czas wynajęcia adresu IP to 24 godziny, zatem wszystkie urządzenia z pliku UDHCPD.leases były podłączone do sieci w ciągu 24 godzin od daty modyfikacji pliku wstecz.



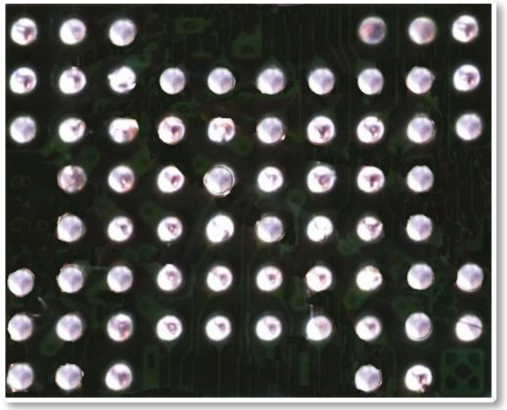
Case 2 – Google Home Speaker

- Urządzenie w pełni kontrolowane głosem
- Spełnia standardowe funkcje smart speakera oraz wspiera funkcje asystenta Google
- Centralne urządzenie sterujące Smart Home
- Kompatybilny z innymi urządzeniami Chromecast

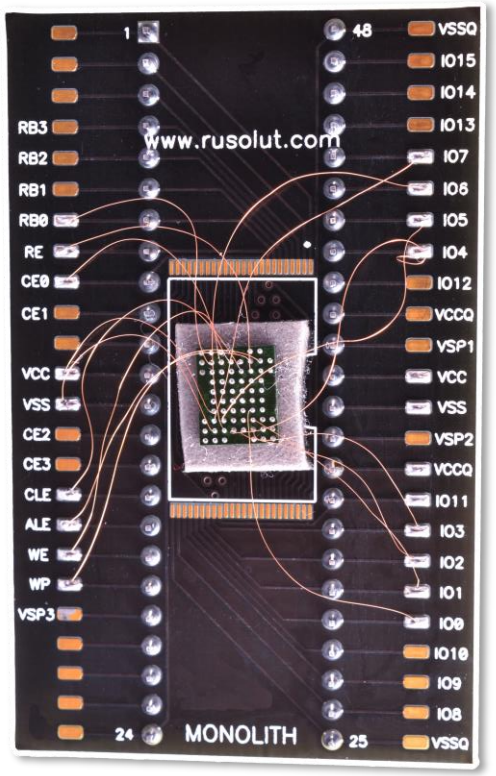
Ekstrakcja chipu pamięci NAND i przygotowanie do odczytu



Unsoldering

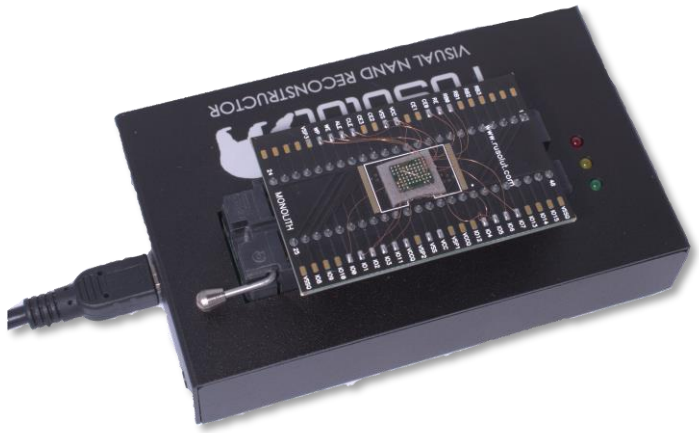


NAND chip

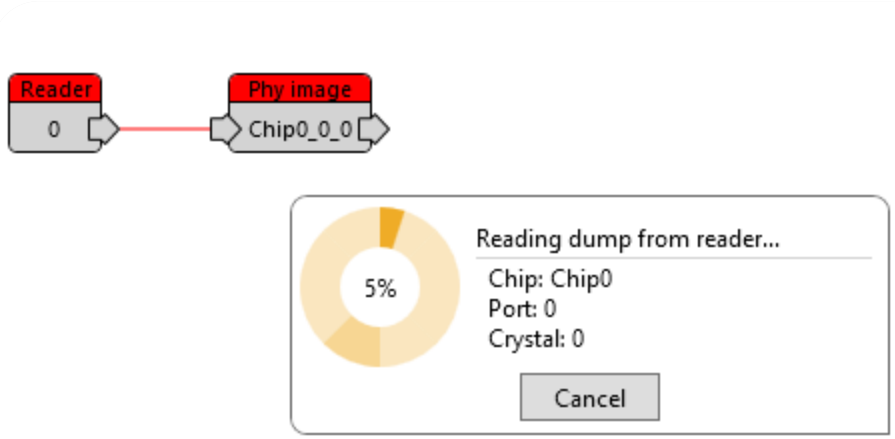


Microsoldering

Odczyt pamięci NAND

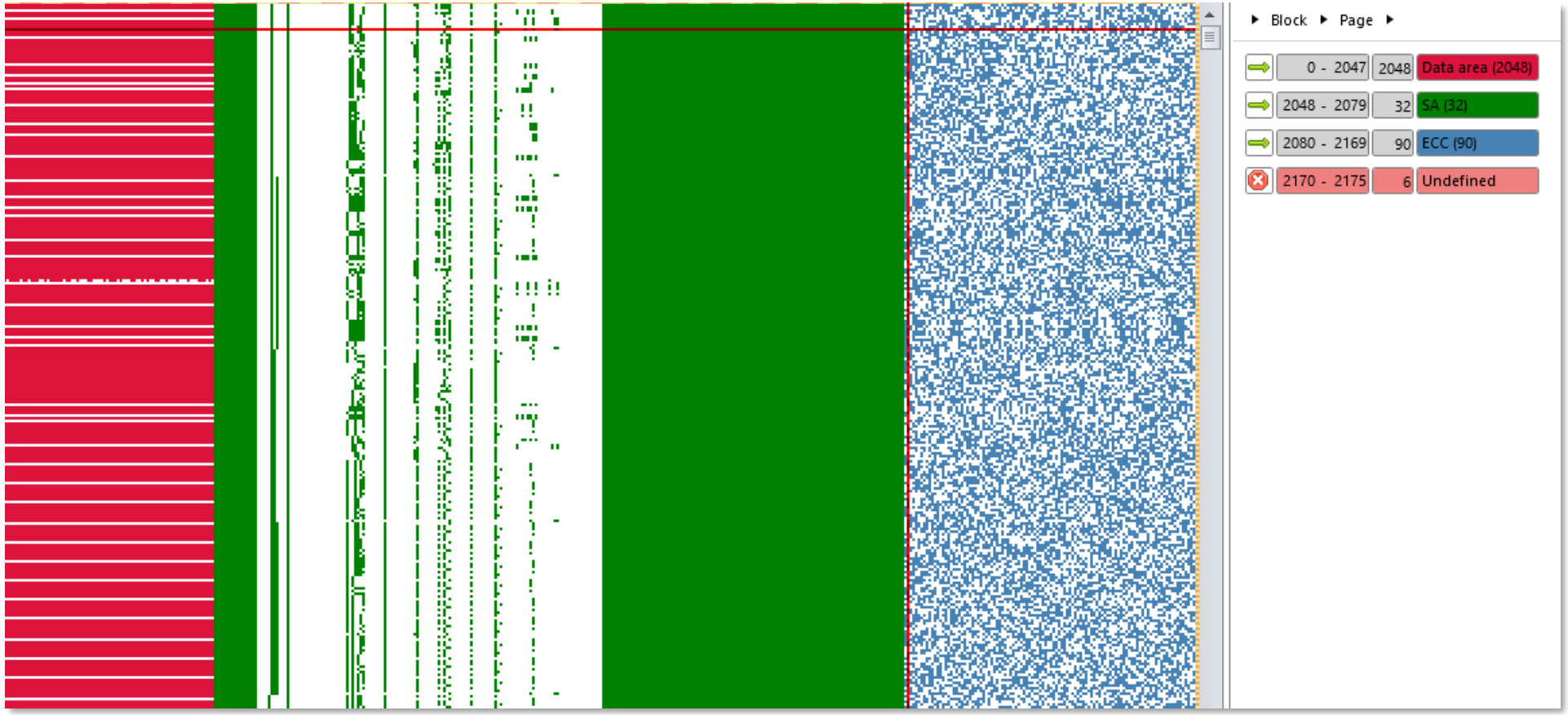


Czytnik VNR z pamięcią NAND



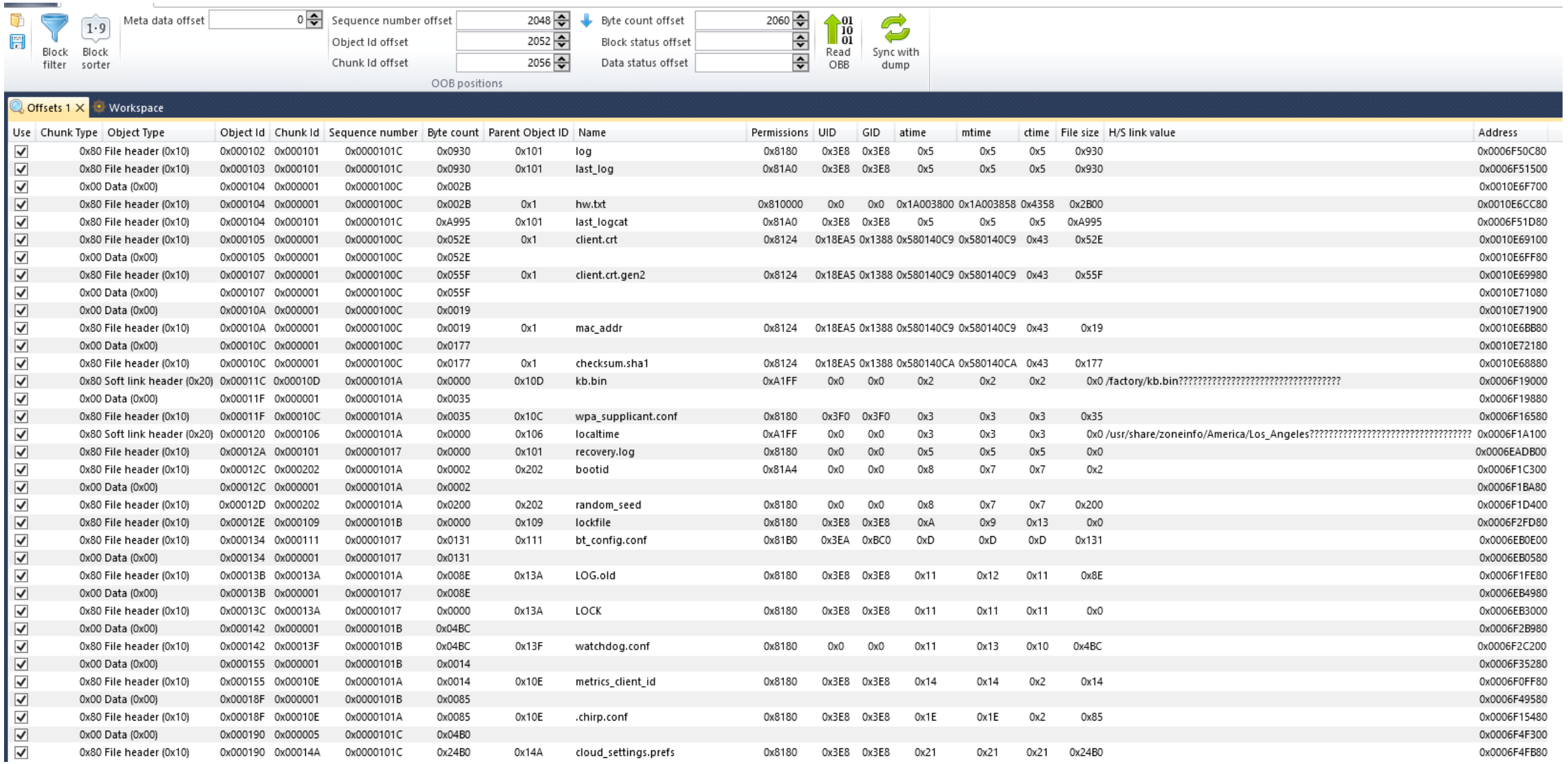
Odczyt pamięci w oprogramowaniu

Wizualna analiza obrazu fizycznego w VNR



Analiza struktury strony

YAFFS Parser - Koncept



Use	Chunk Type	Object Type	Object Id	Chunk Id	Sequence number	Byte count	Parent Object ID	Name	Permissions	UID	GID	atime	mtime	ctime	File size	H/S link value	Address
☑	0x80	File header (0x10)	0x000102	0x000101	0x0000101C	0x0930	0x101	log	0x8180	0x3E8	0x3E8	0x5	0x5	0x5	0x930		0x0006F50C80
☑	0x80	File header (0x10)	0x000103	0x000101	0x0000101C	0x0930	0x101	last_log	0x81A0	0x3E8	0x3E8	0x5	0x5	0x5	0x930		0x0006F51500
☑	0x00	Data (0x00)	0x000104	0x000001	0x0000100C	0x002B											0x0010E6F700
☑	0x80	File header (0x10)	0x000104	0x000001	0x0000100C	0x002B	0x1	hw.txt	0x810000	0x0	0x0	0x1A003800	0x1A003858	0x4358	0x2B00		0x0010E6CC80
☑	0x80	File header (0x10)	0x000104	0x000101	0x0000101C	0xA995	0x101	last_logcat	0x81A0	0x3E8	0x3E8	0x5	0x5	0x5	0xA995		0x0006F51D80
☑	0x80	File header (0x10)	0x000105	0x000001	0x0000100C	0x052E	0x1	client.crt	0x8124	0x18EA5	0x1388	0x580140C9	0x580140C9	0x43	0x52E		0x0010E69100
☑	0x00	Data (0x00)	0x000105	0x000001	0x0000100C	0x052E											0x0010E6FF80
☑	0x80	File header (0x10)	0x000107	0x000001	0x0000100C	0x055F	0x1	client.crt.gen2	0x8124	0x18EA5	0x1388	0x580140C9	0x580140C9	0x43	0x55F		0x0010E69980
☑	0x00	Data (0x00)	0x000107	0x000001	0x0000100C	0x055F											0x0010E71080
☑	0x00	Data (0x00)	0x00010A	0x000001	0x0000100C	0x0019											0x0010E71900
☑	0x80	File header (0x10)	0x00010A	0x000001	0x0000100C	0x0019	0x1	mac_addr	0x8124	0x18EA5	0x1388	0x580140C9	0x580140C9	0x43	0x19		0x0010E6BB80
☑	0x00	Data (0x00)	0x00010C	0x000001	0x0000100C	0x0177											0x0010E72180
☑	0x80	File header (0x10)	0x00010C	0x000001	0x0000100C	0x0177	0x1	checksum.sha1	0x8124	0x18EA5	0x1388	0x580140CA	0x580140CA	0x43	0x177		0x0010E68880
☑	0x80	Soft link header (0x20)	0x00011C	0x00010D	0x0000101A	0x0000	0x10D	kb.bin	0xA1FF	0x0	0x0	0x2	0x2	0x2	0x0	/factory/kb.bin????????????????????????????????	0x0006F19000
☑	0x00	Data (0x00)	0x00011F	0x000001	0x0000101A	0x0035											0x0006F19880
☑	0x80	File header (0x10)	0x00011F	0x00010C	0x0000101A	0x0035	0x10C	wpa_supplicant.conf	0x8180	0x3F0	0x3F0	0x3	0x3	0x3	0x35		0x0006F16580
☑	0x80	Soft link header (0x20)	0x000120	0x000106	0x0000101A	0x0000	0x106	localtime	0xA1FF	0x0	0x0	0x3	0x3	0x3	0x0	/usr/share/zoneinfo/America/Los_Angeles????????????????????????????????	0x0006F1A100
☑	0x80	File header (0x10)	0x00012A	0x000101	0x00001017	0x0000	0x101	recovery.log	0x8180	0x0	0x0	0x5	0x5	0x5	0x0		0x0006EADB00
☑	0x80	File header (0x10)	0x00012C	0x000202	0x0000101A	0x0002	0x202	bootid	0x81A4	0x0	0x0	0x8	0x7	0x7	0x2		0x0006F1C300
☑	0x00	Data (0x00)	0x00012C	0x000001	0x0000101A	0x0002											0x0006F1BA80
☑	0x80	File header (0x10)	0x00012D	0x000202	0x0000101A	0x0200	0x202	random_seed	0x8180	0x0	0x0	0x8	0x7	0x7	0x200		0x0006F1D400
☑	0x80	File header (0x10)	0x00012E	0x000109	0x0000101B	0x0000	0x109	lockfile	0x8180	0x3E8	0x3E8	0xA	0x9	0x13	0x0		0x0006F2FD80
☑	0x80	File header (0x10)	0x000134	0x000111	0x00001017	0x0131	0x111	bt_config.conf	0x81B0	0x3EA	0xBC0	0xD	0xD	0xD	0x131		0x0006EB0E00
☑	0x00	Data (0x00)	0x000134	0x000001	0x00001017	0x0131											0x0006EB0580
☑	0x80	File header (0x10)	0x00013B	0x00013A	0x0000101A	0x008E	0x13A	LOG.old	0x8180	0x3E8	0x3E8	0x11	0x12	0x11	0x8E		0x0006F1FE80
☑	0x00	Data (0x00)	0x00013B	0x000001	0x00001017	0x008E											0x0006EB4980
☑	0x80	File header (0x10)	0x00013C	0x00013A	0x00001017	0x0000	0x13A	LOCK	0x8180	0x3E8	0x3E8	0x11	0x11	0x11	0x0		0x0006EB3000
☑	0x00	Data (0x00)	0x000142	0x000001	0x0000101B	0x04BC											0x0006F2B980
☑	0x80	File header (0x10)	0x000142	0x00013F	0x0000101B	0x04BC	0x13F	watchdog.conf	0x8180	0x0	0x0	0x11	0x13	0x10	0x4BC		0x0006F2C200
☑	0x00	Data (0x00)	0x000155	0x000001	0x0000101B	0x0014											0x0006F35280
☑	0x80	File header (0x10)	0x000155	0x00010E	0x0000101A	0x0014	0x10E	metrics_client_id	0x8180	0x3E8	0x3E8	0x14	0x14	0x2	0x14		0x0006F0FF80
☑	0x00	Data (0x00)	0x00018F	0x000001	0x0000101B	0x0085											0x0006F49580
☑	0x80	File header (0x10)	0x00018F	0x00010E	0x0000101A	0x0085	0x10E	.chirp.conf	0x8180	0x3E8	0x3E8	0x1E	0x1E	0x2	0x85		0x0006F15480
☑	0x00	Data (0x00)	0x000190	0x000005	0x0000101C	0x04B0											0x0006F4F300
☑	0x80	File header (0x10)	0x000190	0x00014A	0x0000101C	0x24B0	0x14A	cloud_settings.prefs	0x8180	0x3E8	0x3E8	0x21	0x21	0x21	0x24B0		0x0006F4FB80

Wyodrębnione pliki z wykorzystaniem YAFFS Parsera

Wyodrębnione pliki z badanego urządzenia #1

- bootid
- bt_config.conf
- build_info.txt
- checksum.sha1
- client.crt
- client.crt.gen2
- cloud_settings.prefs
- eureka.conf
- hw.txt
- LOG
- LOG.old
- mac_addr
- metrics_client_id
- random_seed
- serial.txt
- watchdog.conf

etc.

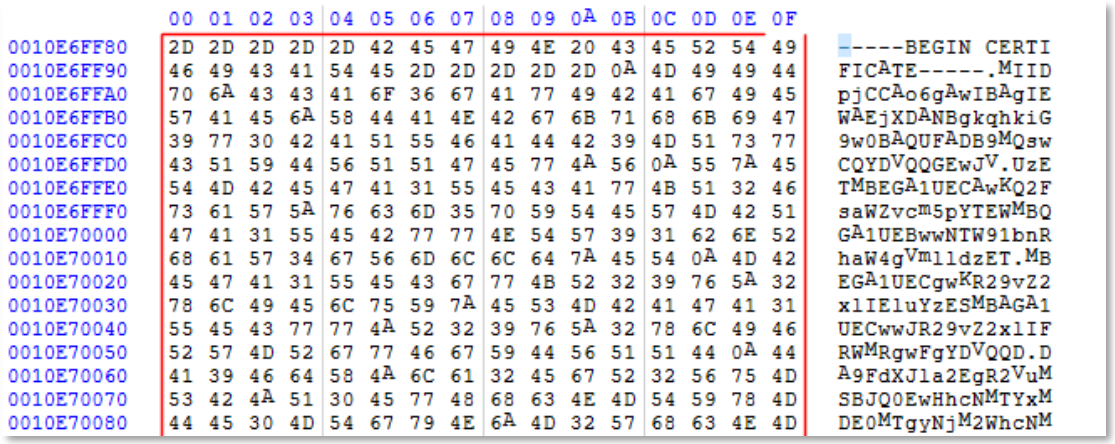
Wyodrębnione pliki z badanego urządzenia #2

- eureka.conf
- watchdog.conf
- hostapd_entropy.bin
- bootid
- pkcs11.txt
- client.crt.gen2
- key4.db
- cert9.db
- metrics_client_id
- ampservice.pid
- test-bin.stderr
- test-bin.stdout
- settings

etc.

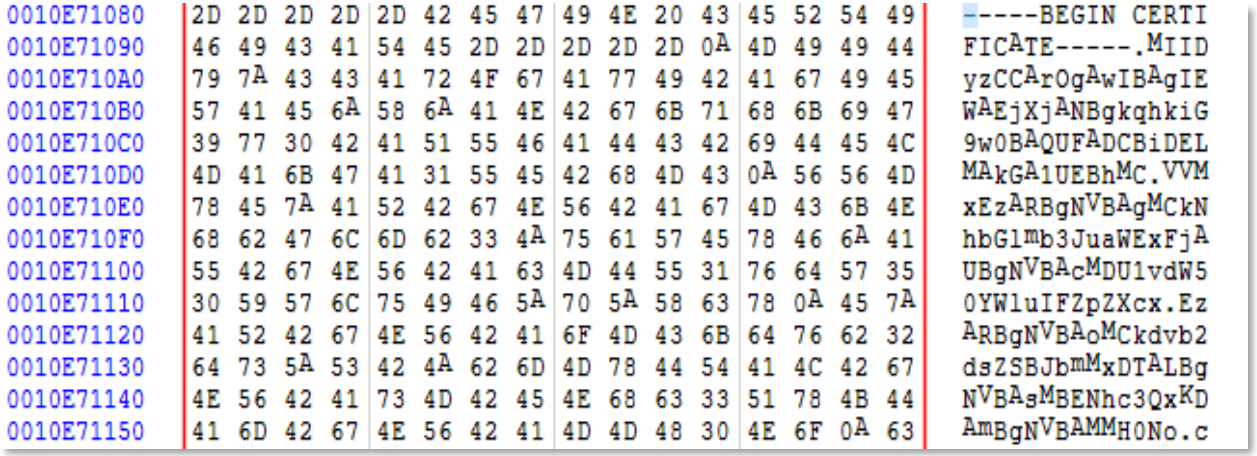
Przykłady uzyskanych plików #1

client.crt
(SSL certificate)



	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
0010E6FF80	2D	2D	2D	2D	2D	42	45	47	49	4E	20	43	45	52	54	49	-----BEGIN CERTI
0010E6FF90	46	49	43	41	54	45	2D	2D	2D	2D	2D	0A	4D	49	49	44	FICATE-----.MIID
0010E6FFA0	70	6A	43	43	41	6F	36	67	41	77	49	42	41	67	49	45	pjCCAo6gAwIBAgIE
0010E6FFB0	57	41	45	6A	58	44	41	4E	42	67	6B	71	68	6B	69	47	WAEjXDANBgkqhkiG
0010E6FFC0	39	77	30	42	41	51	55	46	41	44	42	39	4D	51	73	77	9w0BAQUFADB9MQsw
0010E6FFD0	43	51	59	44	56	51	51	47	45	77	4A	56	0A	55	7A	45	CQYDVQQGEwJV.UzE
0010E6FFE0	54	4D	42	45	47	41	31	55	45	43	41	77	4B	51	32	46	TMBEGA1UECAwKQ2F
0010E6FFF0	73	61	57	5A	76	63	6D	35	70	59	54	45	57	4D	42	51	saWZvcm5pYTEWMBQ
0010E70000	47	41	31	55	45	42	77	77	4E	54	57	39	31	62	6E	52	GA1UEBwwNTW91bnR
0010E70010	68	61	57	34	67	56	6D	6C	6C	64	7A	45	54	0A	4D	42	haW4gVmlldzET.MB
0010E70020	45	47	41	31	55	45	43	67	77	4B	52	32	39	76	5A	32	EGA1UECgwKR29vZ2
0010E70030	78	6C	49	45	6C	75	59	7A	45	53	4D	42	41	47	41	31	xlIEluYzESMBAGA1
0010E70040	55	45	43	77	77	4A	52	32	39	76	5A	32	78	6C	49	46	UECwwJR29vZ2xlIF
0010E70050	52	57	4D	52	67	77	46	67	59	44	56	51	51	44	0A	44	RWMRgwFgYDVQQD.D
0010E70060	41	39	46	64	58	4A	6C	61	32	45	67	52	32	56	75	4D	A9FdXJla2EgR2VuM
0010E70070	53	42	4A	51	30	45	77	48	68	63	4E	4D	54	59	78	4D	SBJQ0EwHhcNMTYxM
0010E70080	44	45	30	4D	54	67	79	4E	6A	4D	32	57	68	63	4E	4D	DE0MTgyNjM2WhcNM

client.crt.gen2
(SSL certificate)



0010E71080	2D	2D	2D	2D	2D	42	45	47	49	4E	20	43	45	52	54	49	-----BEGIN CERTI
0010E71090	46	49	43	41	54	45	2D	2D	2D	2D	2D	0A	4D	49	49	44	FICATE-----.MIID
0010E710A0	79	7A	43	43	41	72	4F	67	41	77	49	42	41	67	49	45	yzCCArOgAwIBAgIE
0010E710B0	57	41	45	6A	58	6A	41	4E	42	67	6B	71	68	6B	69	47	WAEjXjANBgkqhkiG
0010E710C0	39	77	30	42	41	51	55	46	41	44	43	42	69	44	45	4C	9w0BAQUFADCBiDEL
0010E710D0	4D	41	6B	47	41	31	55	45	42	68	4D	43	0A	56	56	4D	MAkGA1UEBhMC.VVM
0010E710E0	78	45	7A	41	52	42	67	4E	56	42	41	67	4D	43	6B	4E	xEzARBgNVBAgMCkN
0010E710F0	68	62	47	6C	6D	62	33	4A	75	61	57	45	78	46	6A	41	hbGlmb3JuaWExFjA
0010E71100	55	42	67	4E	56	42	41	63	4D	44	55	31	76	64	57	35	UBgNVBAcMDU1vdW5
0010E71110	30	59	57	6C	75	49	46	5A	70	5A	58	63	78	0A	45	7A	0YWluIFZpZXcx.Ez
0010E71120	41	52	42	67	4E	56	42	41	6F	4D	43	6B	64	76	62	32	ARBgNVBAoMCkdvb2
0010E71130	64	73	5A	53	42	4A	62	6D	4D	78	44	54	41	4C	42	67	dsZSBJbmMxDTALBg
0010E71140	4E	56	42	41	73	4D	42	45	4E	68	63	33	51	78	4B	44	NVBAsMBENhc3QxKD
0010E71150	41	6D	42	67	4E	56	42	41	4D	4D	48	30	4E	6F	0A	63	AmBgNVBAMMH0No.c

Certyfikat SSL pozwala na odszyfrowanie pełnej komunikacji Smart Speakera.

To jedna z tych sytuacji, w których kryminalistyka znajduje zastosowanie w wywiadzie… Wyobraźmy sobie scenariusz, w którym już posiadamy próbki takiej komunikacji…

Przykłady uzyskanych plików #2

Settings (geolocation)

Offsets 0

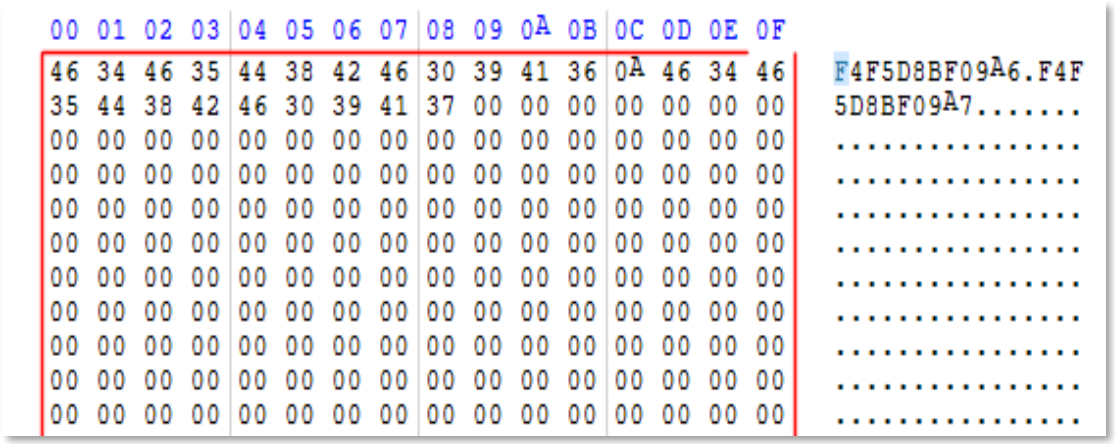
```
          00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
000001DC00 7B 22 67 65 6F 6C 6F 63 61 74 69 6F 6E 22 3A 7B   {"geolocation":{
000001DC10 22 6C 61 74 69 74 75 64 65 22 3A 33 37 2E 33 38   "latitude":37.38
000001DC20 39 34 2C 22 6C 6F 6E 67 69 74 75 64 65 22 3A 2D   94,"longitude":-
000001DC30 31 32 32 2E 30 38 31 39 2C 22 76 61 6C 69 64 22   122.0819,"valid"
000001DC40 3A 74 72 75 65 7D 2C 22 68 6F 74 77 6F 72 64 5F   :true},"hotword_
000001DC50 6E 61 6D 65 22 3A 22 22 2C 22 76 6F 6C 75 6D 65   name":"","volume
000001DC60 5F 69 6E 66 6F 22 3A 7B 22 61 6C 61 72 6D 5F 76   _info":{"alarm_v
000001DC70 6F 6C 75 6D 65 22 3A 30 2E 34 34 39 39 39 39 39   olume":0.4499999
000001DC80 38 38 30 37 39 30 37 31 30 34 2C 22 73 61 76 65   8807907104,"save
000001DC90 64 5F 6E 6F 6E 61 73 73 69 73 74 61 6E 74 5F 76   d_nonassistant_v
000001DCA0 6F 6C 75 6D 65 22 3A 2D 31 2E 30 7D 7D 00 00 00   olume":-1.0}}...
000001DCB0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
000001DCC0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
000001DCD0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
```

metrics_client_id

```
31 37 31 39 31 38 38 33 36 36 31 33 38 37 39 34   1719188366138794
30 38 33 31 00 00 00 00 00 00 00 00 00 00 00 00   0831............
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
```

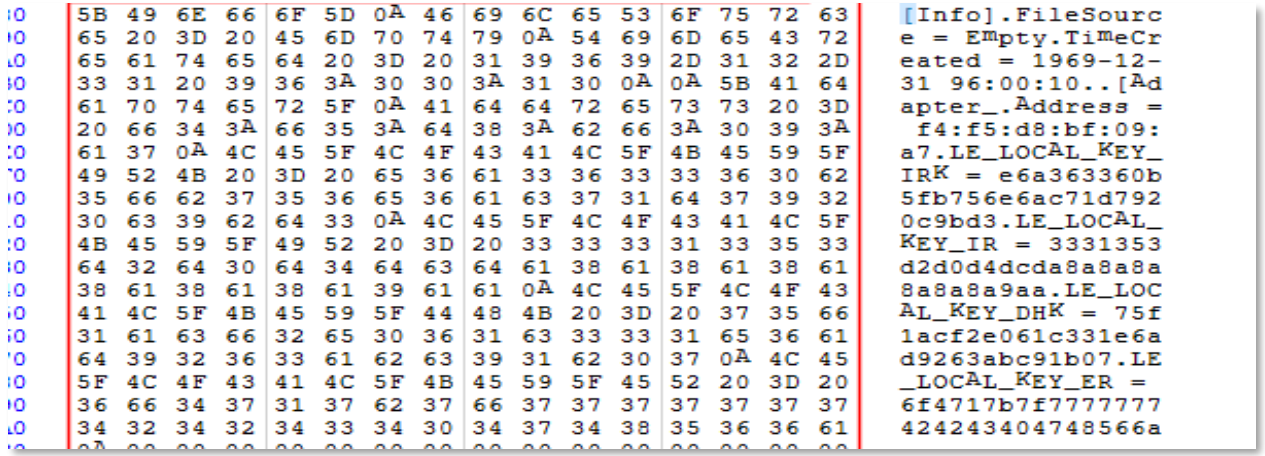
Przykłady uzyskanych plików #3

mac_addr



```
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
46 34 46 35 44 38 42 46 30 39 41 36 0A 46 34 46   F4F5D8BF09A6.F4F
35 44 38 42 46 30 39 41 37 00 00 00 00 00 00 00   5D8BF09A7.......
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
```

bt_config.conf



```
5B 49 6E 66 6F 5D 0A 46 69 6C 65 53 6F 75 72 63   [Info].FileSourc
65 20 3D 20 45 6D 70 74 79 0A 54 69 6D 65 43 72   e = Empty.TimeCr
65 61 74 65 64 20 3D 20 31 39 36 39 2D 31 32 2D   eated = 1969-12-
33 31 20 39 36 3A 30 30 3A 31 30 0A 0A 5B 41 64   31 96:00:10..[Ad
61 70 74 65 72 5F 0A 41 64 64 72 65 73 73 20 3D   apter_.Address =
20 66 34 3A 66 35 3A 64 38 3A 62 66 3A 30 39 3A    f4:f5:d8:bf:09:
61 37 0A 4C 45 5F 4C 4F 43 41 4C 5F 4B 45 59 5F   a7.LE_LOCAL_KEY_
49 52 4B 20 3D 20 65 36 61 33 36 33 33 36 30 62   IRK = e6a363360b
35 66 62 37 35 36 65 36 61 63 37 31 64 37 39 32   5fb756e6ac71d792
30 63 39 62 64 33 0A 4C 45 5F 4C 4F 43 41 4C 5F   0c9bd3.LE_LOCAL_
4B 45 59 5F 49 52 20 3D 20 33 33 33 31 33 35 33   KEY_IR = 3331353
64 32 64 30 64 34 64 63 64 61 38 61 38 61 38 61   d2d0d4dcda8a8a8a
38 61 38 61 38 61 39 61 61 0A 4C 45 5F 4C 4F 43   8a8a8a9aa.LE_LOC
41 4C 5F 4B 45 59 5F 44 48 4B 20 3D 20 37 35 66   AL_KEY_DHK = 75f
31 61 63 66 32 65 30 36 31 63 33 33 31 65 36 61   1acf2e061c331e6a
64 39 32 36 33 61 62 63 39 31 62 30 37 0A 4C 45   d9263abc91b07.LE
5F 4C 4F 43 41 4C 5F 4B 45 59 5F 45 52 20 3D 20   _LOCAL_KEY_ER = 
36 66 34 37 31 37 62 37 66 37 37 37 37 37 37 37   6f4717b7f7777777
34 32 34 32 34 33 34 30 34 37 34 38 35 36 36 61   42424340474856 6a
```

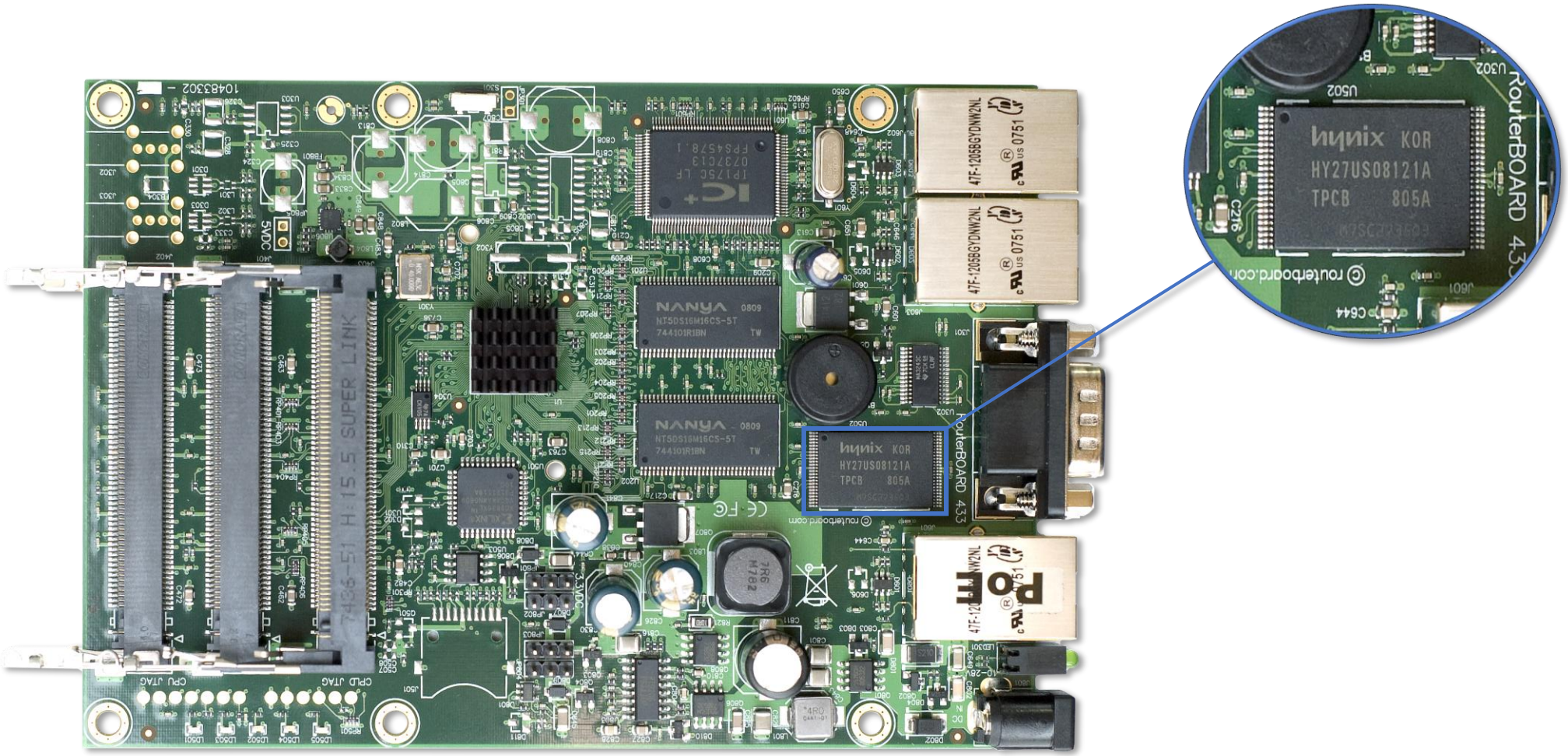
Case 2 - Podsumowanie

Analiza zawartości pamięci Speakera pokazała, że urządzenie nie było ekstensywnie używane i nie było tam zbyt wielu pozostawionych "śladów" użytkownika. Jednakże, tak jak w innych przypadkach połączenie tych informacji wraz z danymi uzyskanymi z telefonu lub innego urządzenia może rzucić nieco światła na badaną sprawę.

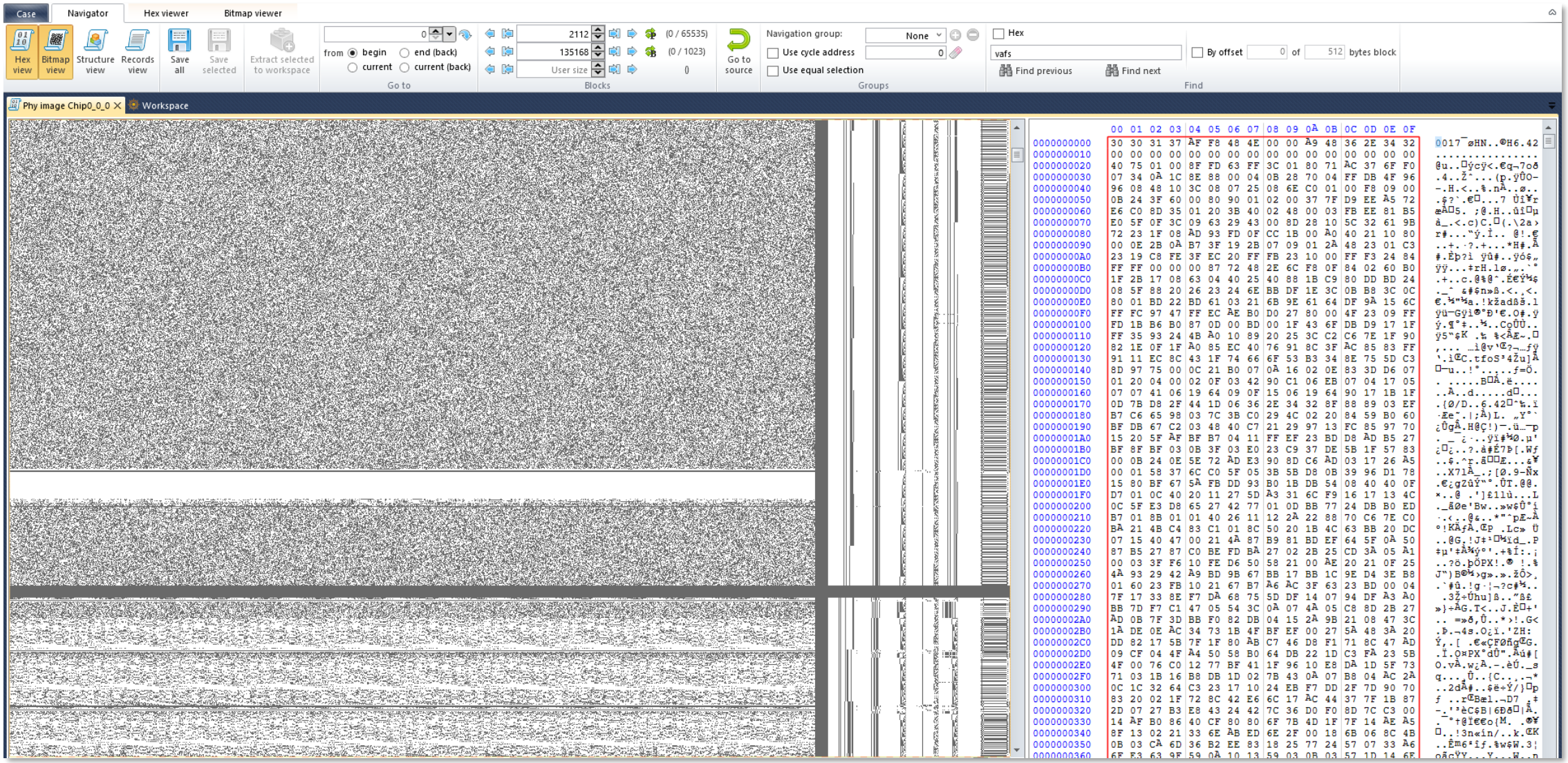
Badania nad tymi urządzeniami w dalszym ciągu trwają. Zebraliśmy obecnie dużo danych z kilku identycznych urządzeń, aby oszacować pełną skalę przechowywanych tam danych oraz możliwości ich połączenia.

Case 3 - Mikrotik RB433GL

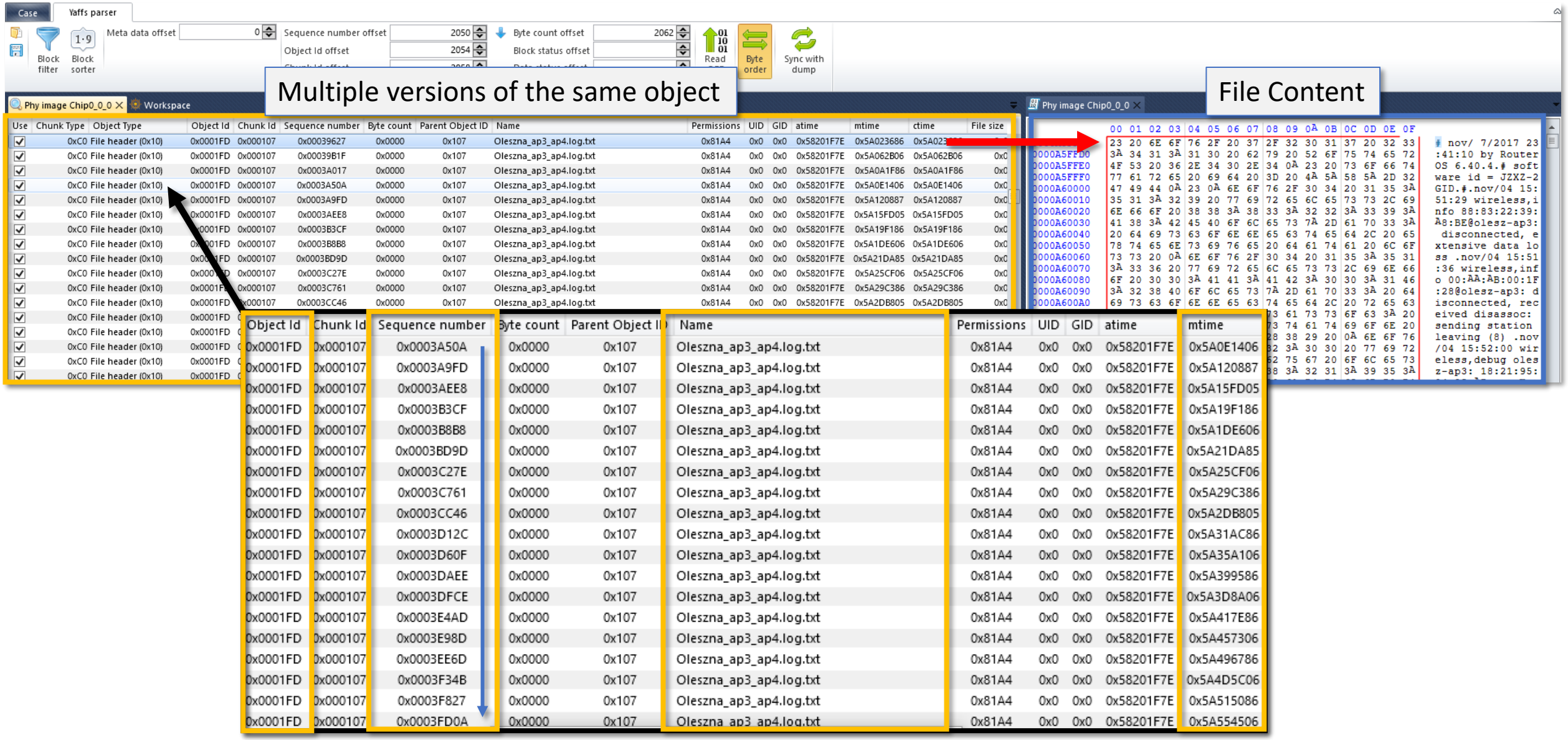
Urządzenie przywrócone do ustawień fabrycznych



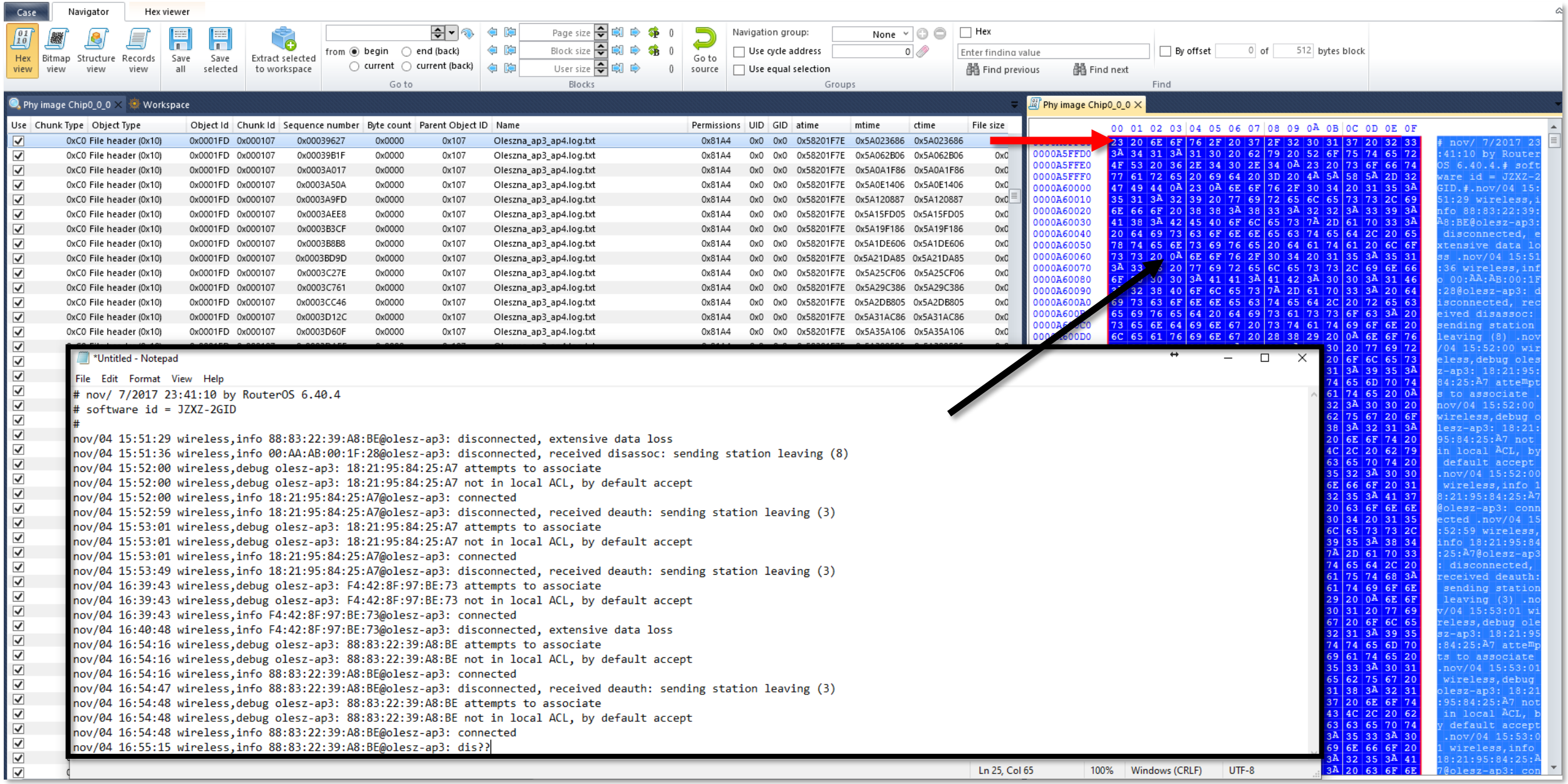
YAFFS2 File system



Parsed YAFFS file system

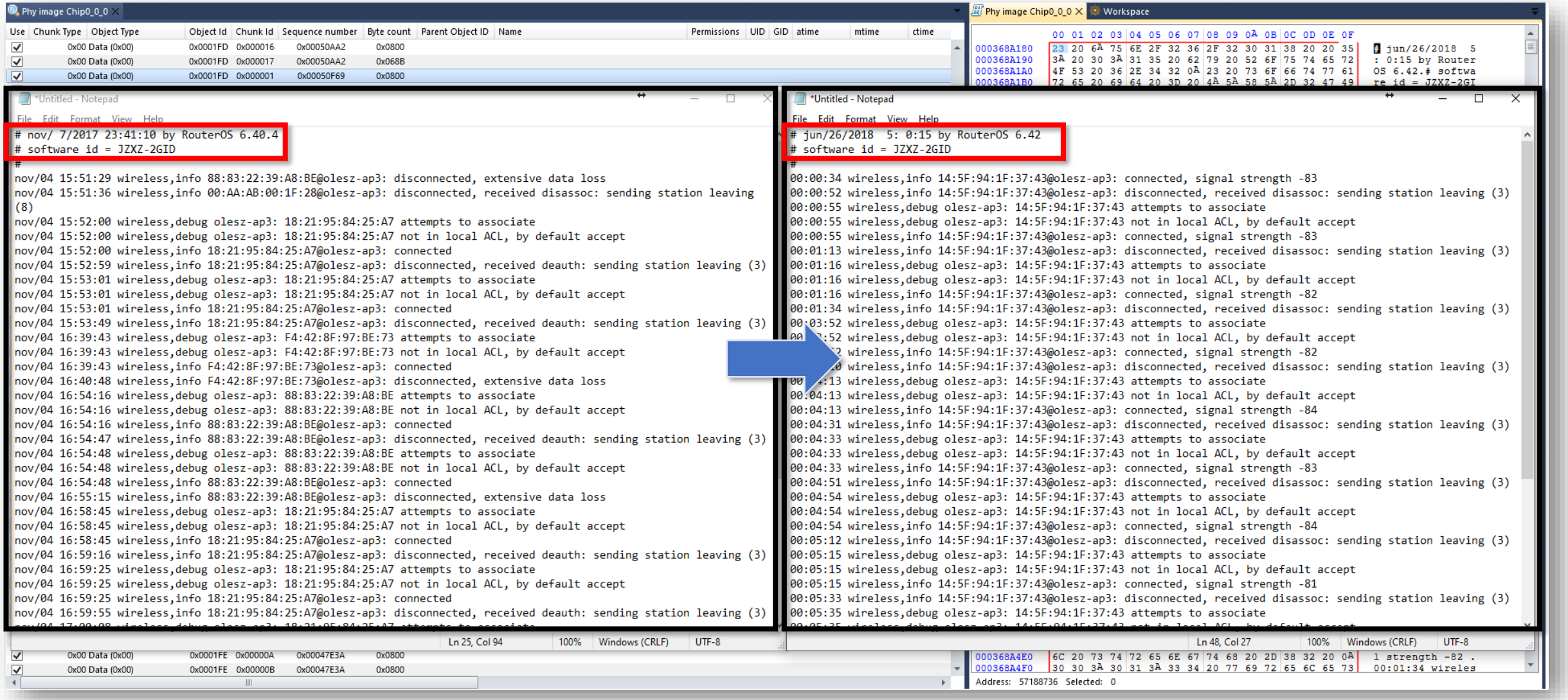


Zawartość obiektu



Case 3 - Podsumowanie

Uzyskany dostęp do pełnej historii logów systemowych z okresu między 07.11.2017 – 26.06.2018



Dziękujemy!

www.rusolut.com
Polczynska 10,
Warsaw, Poland
+48 535 054 431
info@rusolut.com
13-15.06, 2022 Gdynia