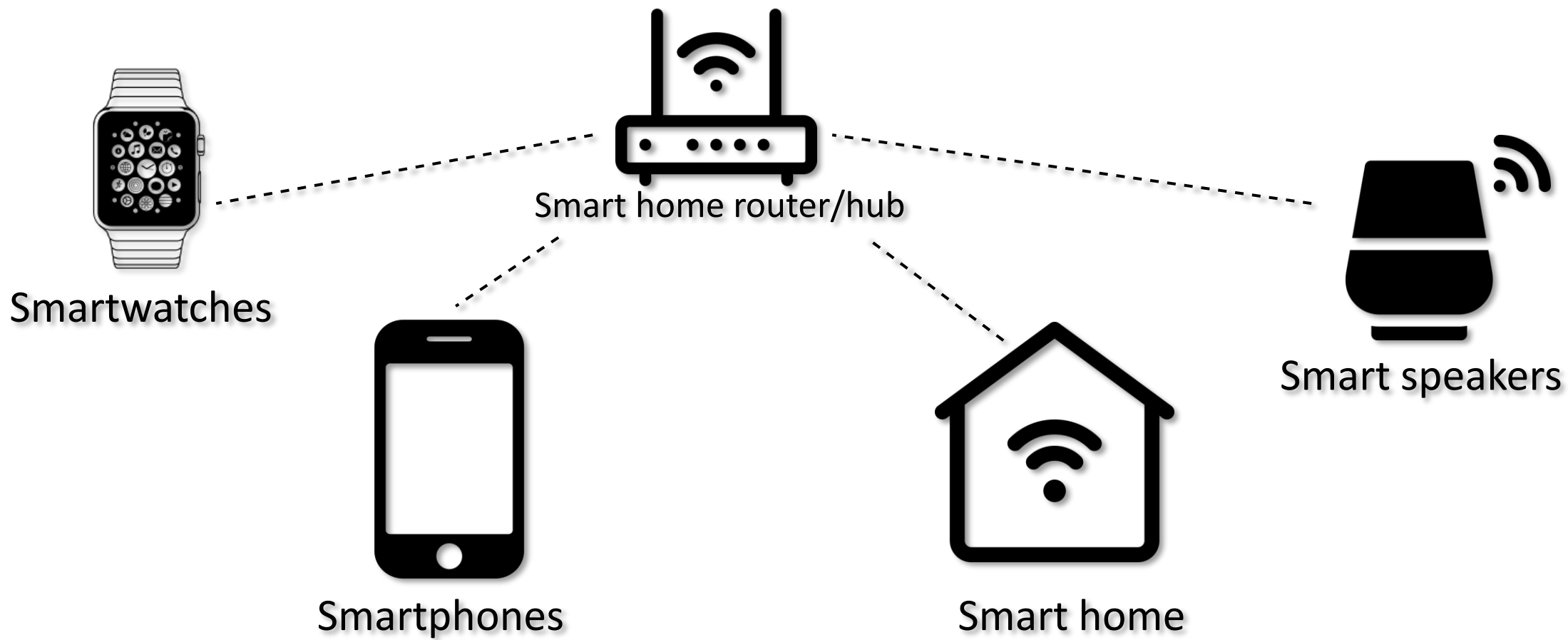


Ekstrakcja dowodów z urządzeń IoT z wykorzystaniem metody Chip-off

Michał Gmurek – Rusolut, Poland

Urządzenia IoT

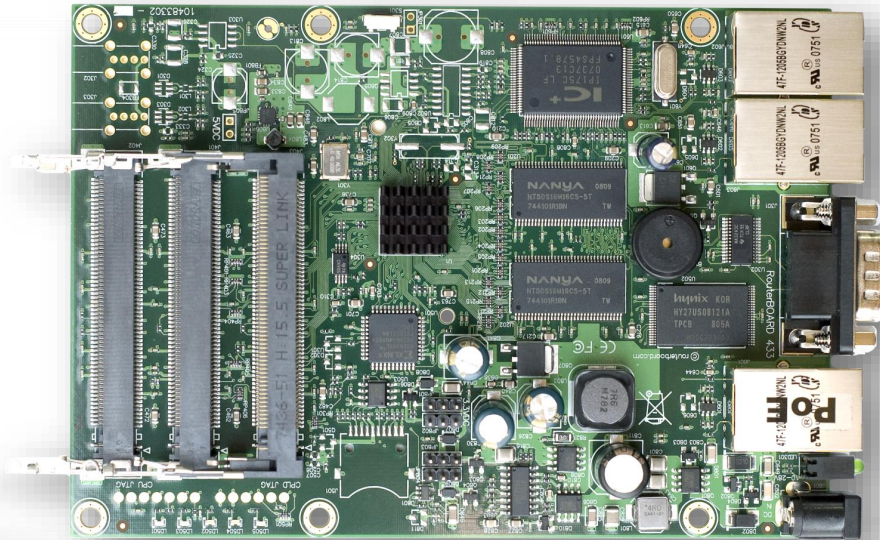


Badane urządzenia

CALIX 844E-1



Mikrotik RB433GL

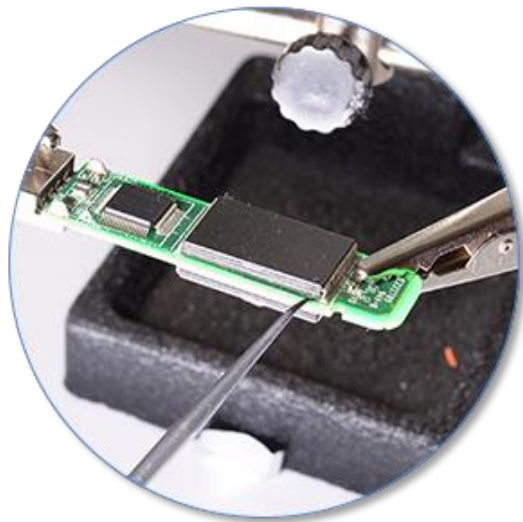


**Google Home
Speaker**

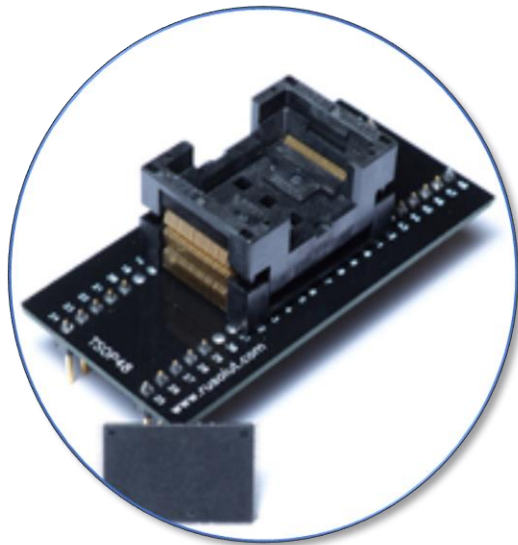


Odzyskiwanie danych metodą Chip-off

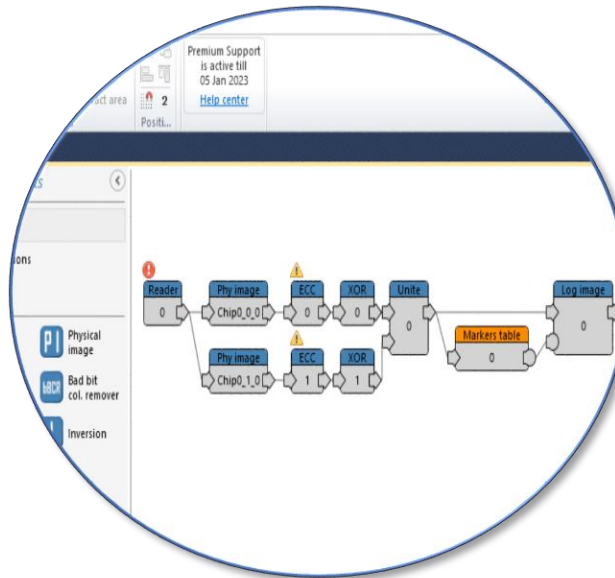
Wylutowanie kości
pamięci NAND



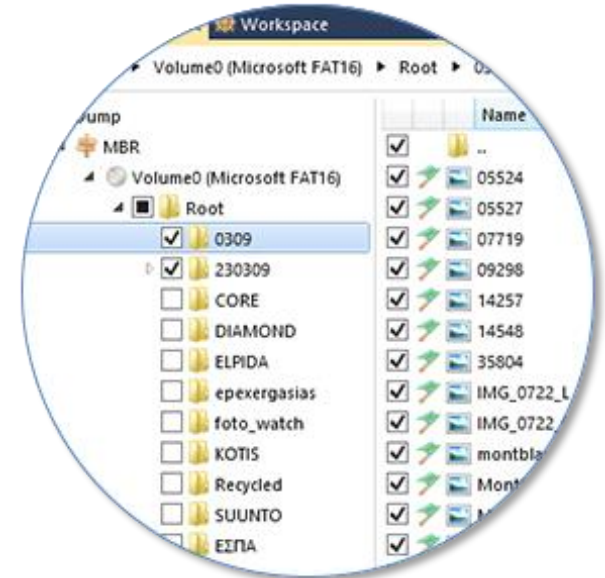
Identyfikacja chipu
oraz dobór adaptera



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

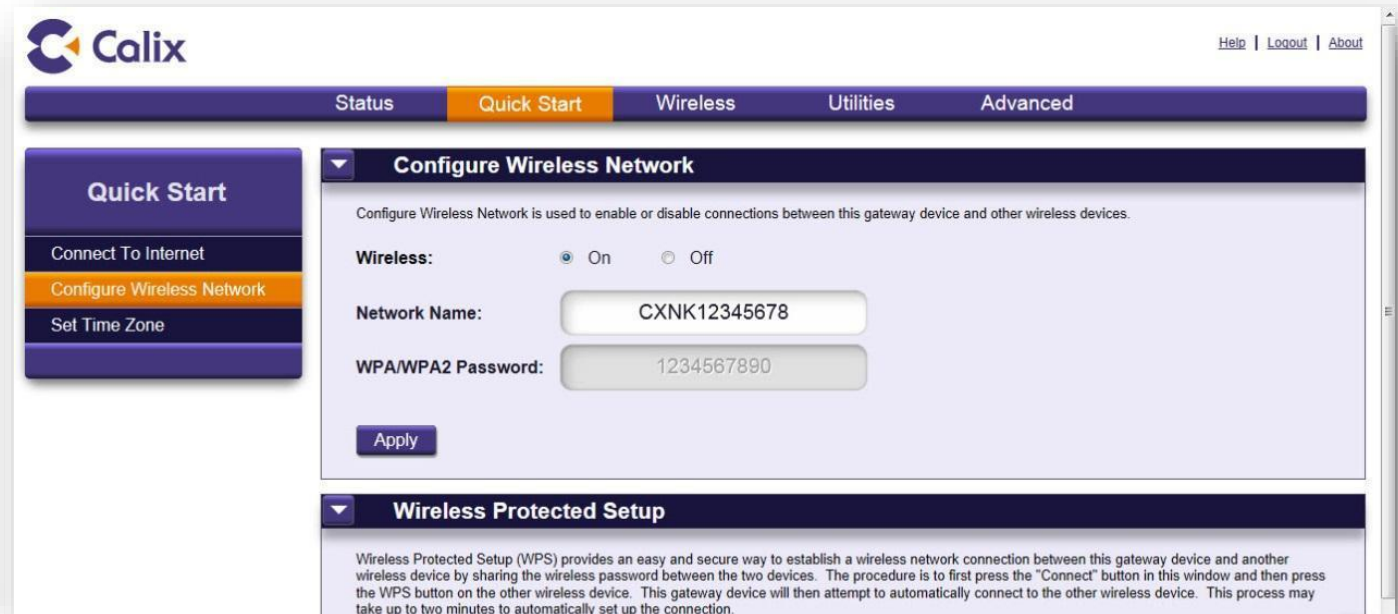
- Wiele wersji systemów pliku
- Brak ustandaryzowanych metadanych
- Możliwości odzyskiwania starych/skasowanych danych

Case 1 - CALIX 844E-1



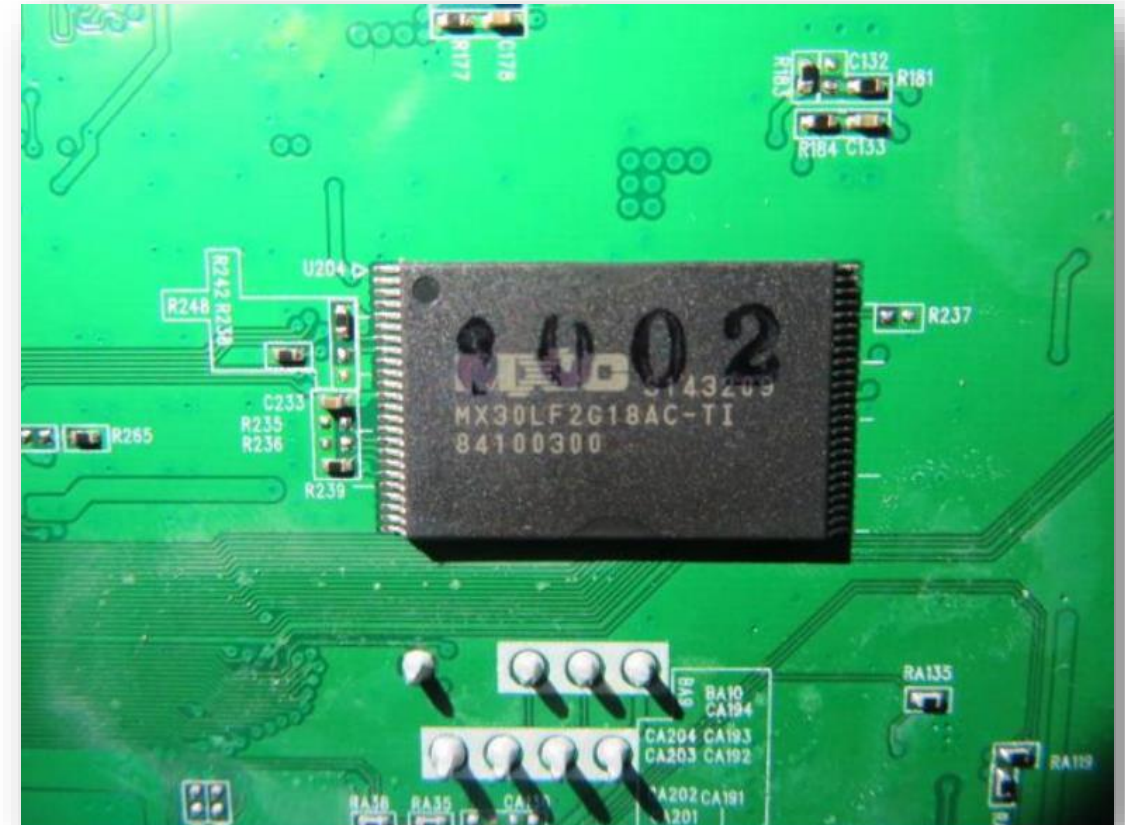
CALIX 844E-1

Oprogramowanie sieciowe



CALIX 844E-1

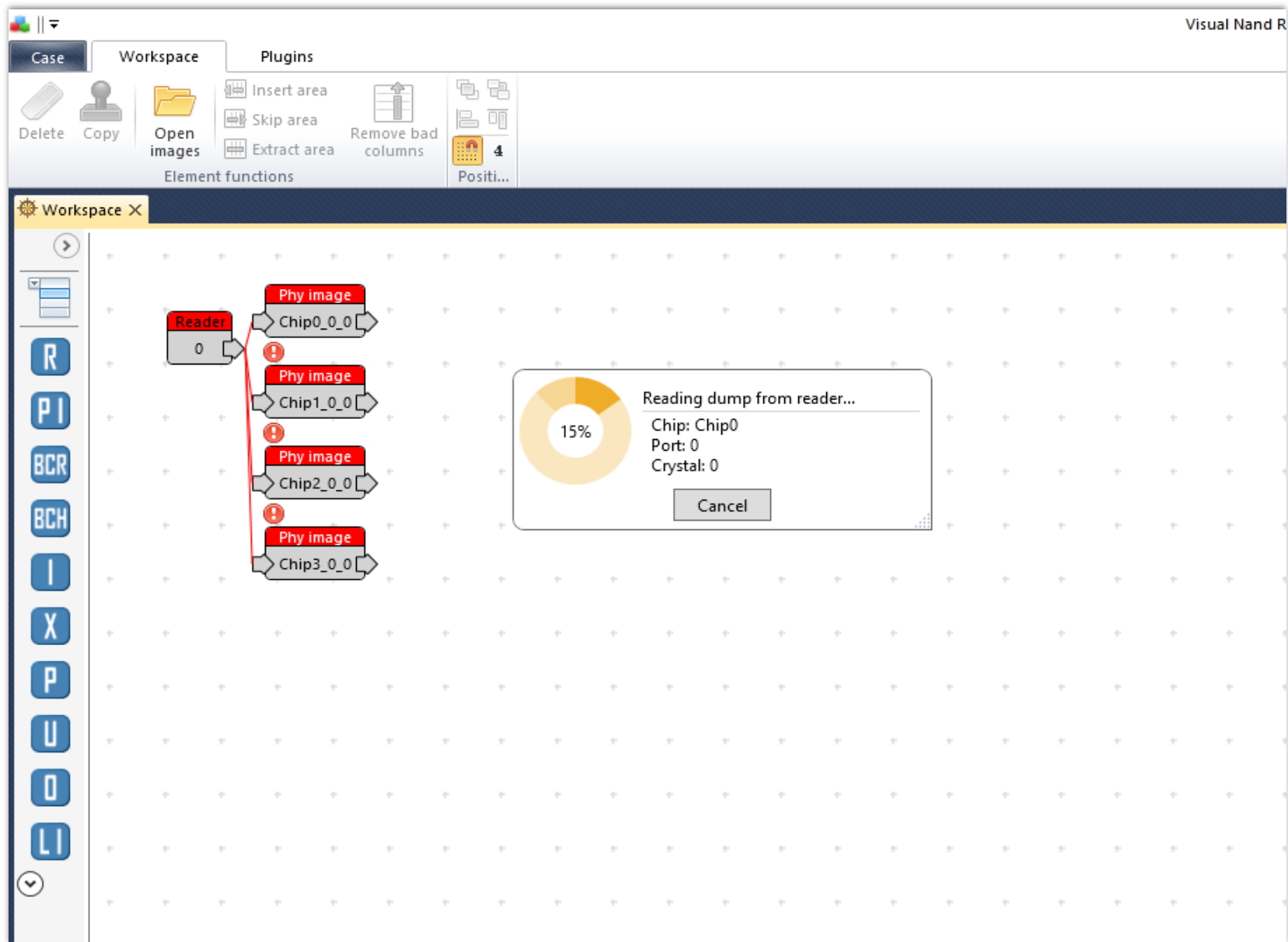
PCB



Odczyt zawartości kości pamięci w VNR



Proces czytania pamięci NAND



Wyczytany obraz fizyczny

Visual Nand Reconstructor

Case Navigator Hex viewer Bitmap viewer

Hex view Bitmap view Structure view Records view Save all Save selected Extract selected to workspace

Page size: 2112 Pixel size: 2 Shift size: 0

Highlight blocks Show structure Show position Show bits statistics Bit order

Start: V 0 H 0 Stop: V 0 H 0 Selected: V 1 H 1

Selection markers

Offsets 2 X Workspace

00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000 55 42 49 23 01 00 00 00 00 00 00 00 00 00 00 01 UBI#.....
00000001 00 00 08 00 00 00 10 00 5E 22 E9 C5 00 00 00 00^"eA..
00000002 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000003 00 00 00 00 00 00 00 00 00 00 00 00 7B A8 C0 D6{~AO..
00000004 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000005 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000006 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000007 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000008 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000009 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000000A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000000B 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000000C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000000D 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000000E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000000F 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000011 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000012 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000013 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000014 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000015 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000016 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000017 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000018 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000019 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000001A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000001B 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000001C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000001D 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000001E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000001F 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000021 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000022 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000023 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000024 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000025 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000026 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000027 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000028 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000029 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000002A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000002B 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000002C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000002D 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000002E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000002F 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000031 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000032 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000033 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000034 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000035 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000036 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

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

Diagram illustrating the structure of DHCP leases and their configuration in a DHCP server configuration file.

The main table displays DHCP lease data, organized into columns:

- MAC Addresses:** The first column lists MAC addresses (e.g., C8 52 61, 18 9C 27).
- Leased IP Addresses:** The second column lists the leased IP addresses (e.g., 192.168.250.10, 192.168.250.11).
- Device name:** The third column lists the device names (e.g., QqDVR_WIFI_18:9c:27, iPhone, Oliver).

A single record is highlighted, showing the mapping of a MAC address to an IP address and a device name.

The configuration file (udhcpd.conf) shows the corresponding configuration for the highlighted record:

```
File Edit Format View Help
decline_file /var/udhcpd.decline
auto_time 900
interface br0
start 192.168.250.10
end 192.168.250.200
option lease 86400
min_lease 30
option subnet 255.255.255.0
option router 192.168.250.1
option dns 192.168.250.1
option domain Home
interface brqt
start 169.254.1.2
end 169.254.1.2
option lease 86400
min_lease 30
option subnet 255.255.255.0
option router 169.254.1.1
option dns 169.254.1.1
option dns 169.254.1.1
option domain Home
```

The configuration file is divided into two sections, one for interface br0 and one for interface brqt. The lease time is set to 86400 seconds (24 hours) for both interfaces.

05/08/2021 01:31:34
Data modyfikacji pliku

Lease time - 24 Hours

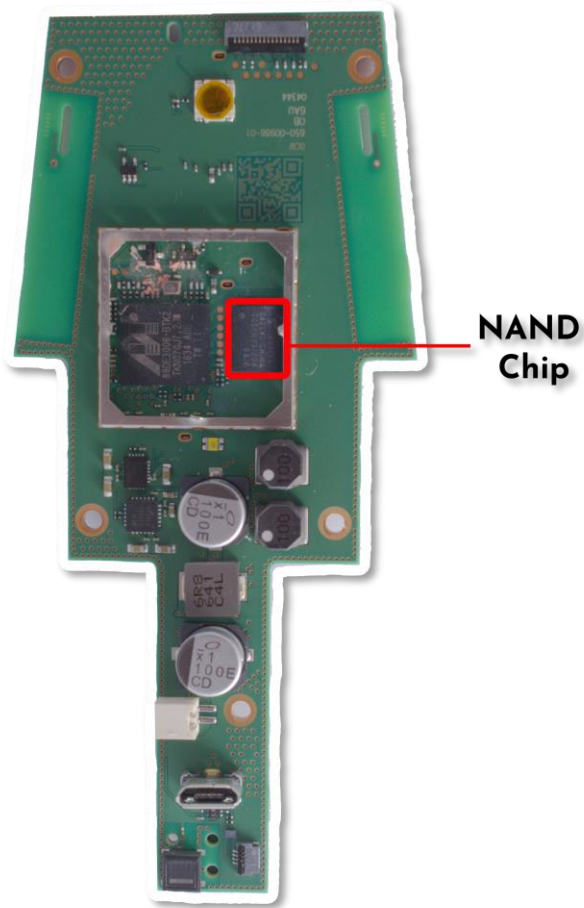
Lease time – 24 Hours

Case 2 – Google Home Speaker

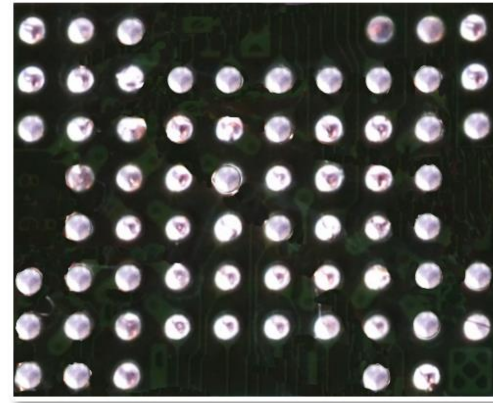


- Urządzenie w pełni kontrolowane głosem
- Spełnia standardowe funkcje smart speakera oraz wspiera funkcje asystenta Google
- Centralne urządzenie sterujące Smart Home
- Kompatybilny z innymi urządzeniami Chromecast

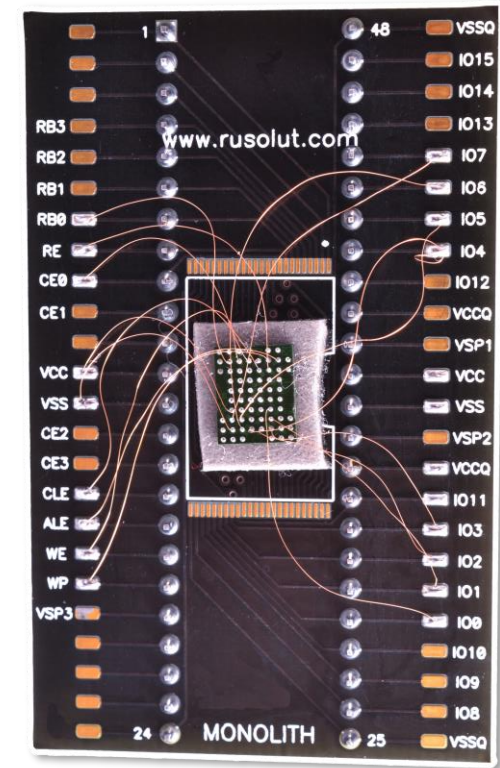
Ekstrakcja chipu pamięci NAND i przygotowanie do odczytu



Unsoldering

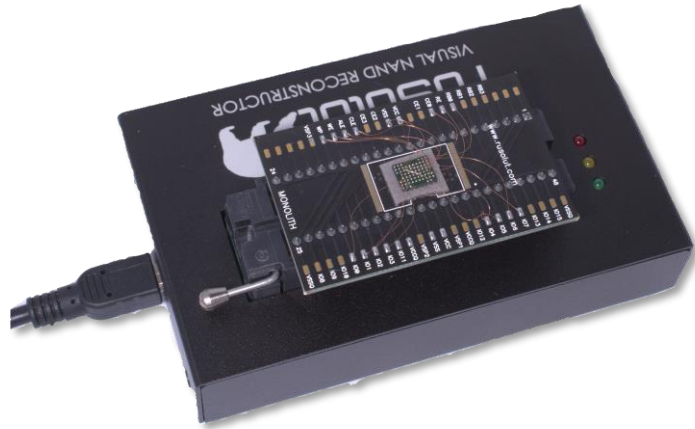


NAND chip

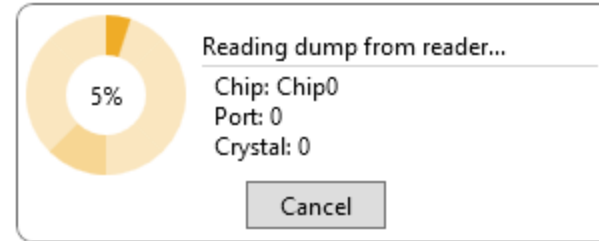


Microsoldering

Odczyt pamięci NAND

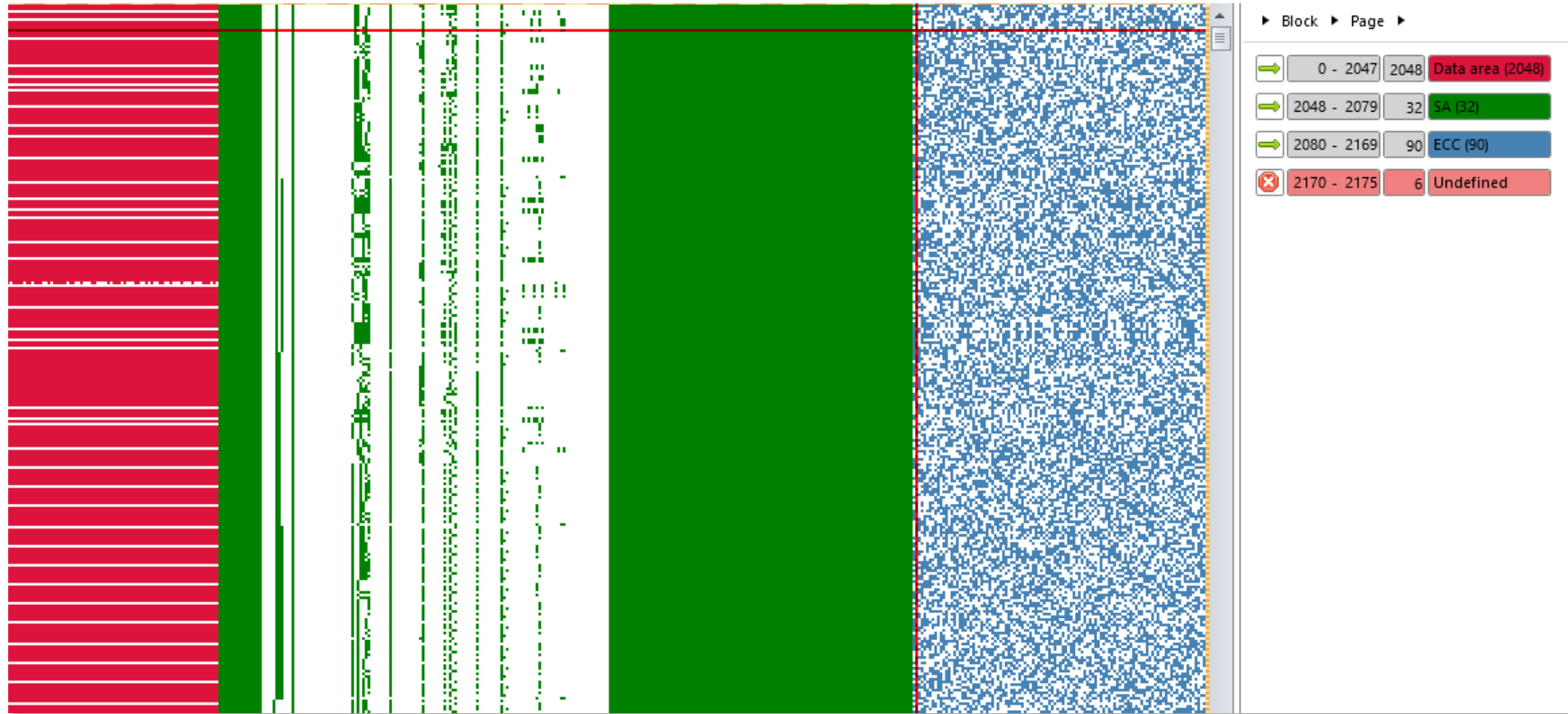


Czytnik VNR z pamięcią NAND



Odczyt pamięci w oprogramowaniu

Wizualna analiza obrazu fizycznego w VNR



Analiza struktury strony

YAFFS Parser - Konzept

		Meta data offset	0	Sequence number offset	2048	Byte count offset	2060										
Block filter	Block sorter			Object Id offset	2052	Block status offset		Read OBB	Sync with dump								
				Chunk Id offset	2056	Data status offset											
OOB positions																	
Offsets 1 X Workspace																	
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	WAEjXjANBgkqhkiG
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	haW4gVm1ldzET.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	x1IEluYzESMBAgA1
0010E70040	55	45	43	77	77	4A	52	32	39	76	5A	32	78	6C	49	46	UECwwJR29vZ2x1IF
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	SBJQOEwHhcNMTYxM
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	xEzARBgNVBAgMcKkN
0010E710F0	68	62	47	6C	6D	62	33	4A	75	61	57	45	78	46	6A	41	hbG1mb3JuaWEwFjA
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...

bt_config.conf

[illegible]

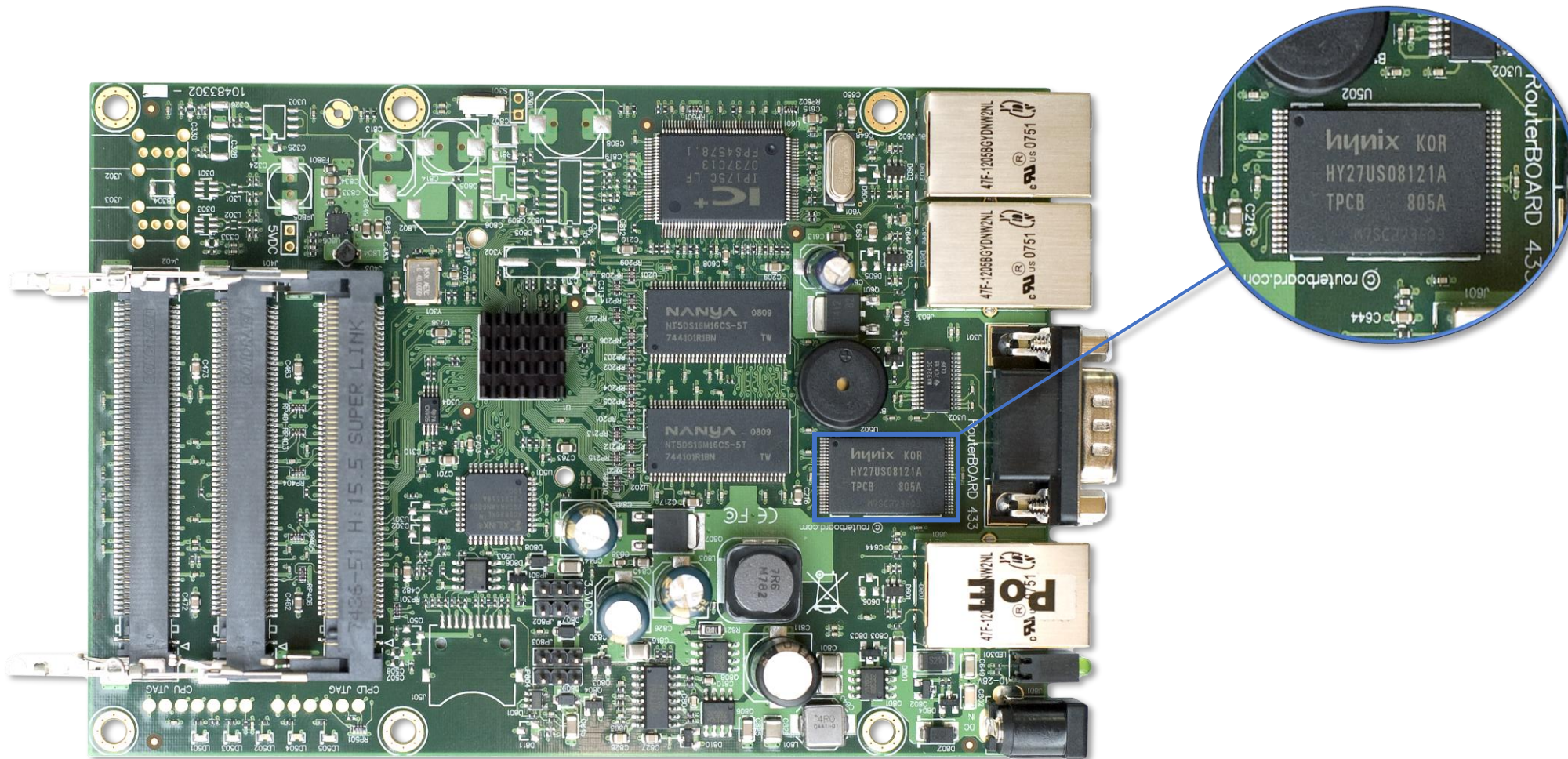
Case 2 - Podsumowanie

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

The screenshot displays a hex editor interface with the following components:

- Menu Bar:** Case, Navigator, Hex viewer, Bitmap viewer.
- Toolbar:** Hex view, Bitmap view, Structure view, Records view, Save all, Save selected, Extract selected to workspace.
- Navigation Panel:** from ☒ begin ☐ end (back) ☐ current ☐ current (back). Go to: 2112. Blocks: 135168 (0 / 65535). User size: 0.
- Navigation group:** None. Use cycle address: ☐. Use equal selection: ☐.
- Find Panel:** Hex, vafs, Find previous, Find next, By offset: 0 of 512 bytes block.
- Workspace:** Phy Image Chip0_0_0 X. The main area shows a large hex dump of data, with a vertical cursor at address 2112. The hex dump shows a series of 0x00 bytes followed by a sequence of data bytes starting with 0x30, 0x30, 0x31, 0x37, etc. The right side of the hex dump shows the corresponding ASCII representation of the data, which appears to be a corrupted or encrypted string.

Parsed YAFFS file system

Case Yaffs parser

Meta data offset: 0 Sequence number offset: 2050 Byte count offset: 2062

Object Id offset: 2054 Block status offset: 2058

Block filter: 1-9 Block sorter

Read Byte order Sync with dump

Multiple versions of the same object

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
✓	0xC0	File header (0x10)	0x0001FD	0x000107	0x00039627	0x0000	0x107	Oleszna_ap3_ap4.log.txt	0x81A4	0x0	0x0	0x58201F7E	0x5A023686	0x5A023686	0x0
✓	0xC0	File header (0x10)	0x0001FD	0x000107	0x00039B1F	0x0000	0x107	Oleszna_ap3_ap4.log.txt	0x81A4	0x0	0x0	0x58201F7E	0x5A062B06	0x5A062B06	0x0
✓	0xC0	File header (0x10)	0x0001FD	0x000107	0x0003A017	0x0000	0x107	Oleszna_ap3_ap4.log.txt	0x81A4	0x0	0x0	0x58201F7E	0x5A0A1F86	0x5A0A1F86	0x0
✓	0xC0	File header (0x10)	0x0001FD	0x000107	0x0003A50A	0x0000	0x107	Oleszna_ap3_ap4.log.txt	0x81A4	0x0	0x0	0x58201F7E	0x5A0E1406	0x5A0E1406	0x0
✓	0xC0	File header (0x10)	0x0001FD	0x000107	0x0003A9FD	0x0000	0x107	Oleszna_ap3_ap4.log.txt	0x81A4	0x0	0x0	0x58201F7E	0x5A120887	0x5A120887	0x0
✓	0xC0	File header (0x10)	0x0001FD	0x000107	0x0003AEE8	0x0000	0x107	Oleszna_ap3_ap4.log.txt	0x81A4	0x0	0x0	0x58201F7E	0x5A15FD05	0x5A15FD05	0x0
✓	0xC0	File header (0x10)	0x0001FD	0x000107	0x0003B3CF	0x0000	0x107	Oleszna_ap3_ap4.log.txt	0x81A4	0x0	0x0	0x58201F7E	0x5A19F186	0x5A19F186	0x0
✓	0xC0	File header (0x10)	0x0001FD	0x000107	0x0003B8B8	0x0000	0x107	Oleszna_ap3_ap4.log.txt	0x81A4	0x0	0x0	0x58201F7E	0x5A1DE606	0x5A1DE606	0x0
✓	0xC0	File header (0x10)	0x0001FD	0x000107	0x0003BD9D	0x0000	0x107	Oleszna_ap3_ap4.log.txt	0x81A4	0x0	0x0	0x58201F7E	0x5A21DA85	0x5A21DA85	0x0
✓	0xC0	File header (0x10)	0x0001FD	0x000107	0x0003C27E	0x0000	0x107	Oleszna_ap3_ap4.log.txt	0x81A4	0x0	0x0	0x58201F7E	0x5A25CF06	0x5A25CF06	0x0
✓	0xC0	File header (0x10)	0x0001FD	0x000107	0x0003C761	0x0000	0x107	Oleszna_ap3_ap4.log.txt	0x81A4	0x0	0x0	0x58201F7E	0x5A29C386	0x5A29C386	0x0
✓	0xC0	File header (0x10)	0x0001FD	0x000107	0x0003CC46	0x0000	0x107	Oleszna_ap3_ap4.log.txt	0x81A4	0x0	0x0	0x58201F7E	0x5A2DB805	0x5A2DB805	0x0
✓	0xC0	File header (0x10)	0x0001FD	0x000107	0x0003D12C	0x0000	0x107	Oleszna_ap3_ap4.log.txt	0x81A4	0x0	0x0	0x58201F7E	0x5A31AC86	0x5A31AC86	0x0
✓	0xC0	File header (0x10)	0x0001FD	0x000107	0x0003D60F	0x0000	0x107	Oleszna_ap3_ap4.log.txt	0x81A4	0x0	0x0	0x58201F7E	0x5A35A106	0x5A35A106	0x0
✓	0xC0	File header (0x10)	0x0001FD	0x000107	0x0003DAEE	0x0000	0x107	Oleszna_ap3_ap4.log.txt	0x81A4	0x0	0x0	0x58201F7E	0x5A399586	0x5A399586	0x0
✓	0xC0	File header (0x10)	0x0001FD	0x000107	0x0003DFCE	0x0000	0x107	Oleszna_ap3_ap4.log.txt	0x81A4	0x0	0x0	0x58201F7E	0x5A3D8A06	0x5A3D8A06	0x0
✓	0xC0	File header (0x10)	0x0001FD	0x000107	0x0003E4AD	0x0000	0x107	Oleszna_ap3_ap4.log.txt	0x81A4	0x0	0x0	0x58201F7E	0x5A417E86	0x5A417E86	0x0
✓	0xC0	File header (0x10)	0x0001FD	0x000107	0x0003E98D	0x0000	0x107	Oleszna_ap3_ap4.log.txt	0x81A4	0x0	0x0	0x58201F7E	0x5A457306	0x5A457306	0x0
✓	0xC0	File header (0x10)	0x0001FD	0x000107	0x0003EE6D	0x0000	0x107	Oleszna_ap3_ap4.log.txt	0x81A4	0x0	0x0	0x58201F7E	0x5A496786	0x5A496786	0x0
✓	0xC0	File header (0x10)	0x0001FD	0x000107	0x0003F34B	0x0000	0x107	Oleszna_ap3_ap4.log.txt	0x81A4	0x0	0x0	0x58201F7E	0x5A4D5C06	0x5A4D5C06	0x0
✓	0xC0	File header (0x10)	0x0001FD	0x000107	0x0003F827	0x0000	0x107	Oleszna_ap3_ap4.log.txt	0x81A4	0x0	0x0	0x58201F7E	0x5A515086	0x5A515086	0x0
✓	0xC0	File header (0x10)	0x0001FD	0x000107	0x0003FD0A	0x0000	0x107	Oleszna_ap3_ap4.log.txt	0x81A4	0x0	0x0	0x58201F7E	0x5A554506	0x5A554506	0x0

File Content

00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
23	20	6E	6F	76	2F	20	37	2F	32	30	31	37	20	32	33
3A	34	31	3A	31	30	20	62	79	20	52	6F	75	74	65	72
4F	53	20	36	2E	34	30	2E	34	0A	23	20	73	6F	66	74
77	61	72	65	20	69	64	20	3D	20	4A	5A	58	5A	2D	32
47	49	44	0A	23	0A	6E	6F	76	2F	30	34	20	31	35	3A
35	31	3A	32	39	20	77	69	72	65	6C	65	73	73	2C	69
6E	66	6F	20	38	38	3A	38	33	3A	32	32	3A	33	39	3A
41	38	3A	42	45	40	6F	6C	65	73	7A	2D	61	70	33	3A
20	64	69	73	63	6F	6E	6E	65	63	74	65	64	2C	20	65
78	74	65	6E	73	69	76	65	20	64	61	74	61	20	6C	6F
73	73	20	0A	6E	6F	76	2F	30	34	20	31	35	3A	35	31
3A	33	36	20	77	69	72	65	6C	65	73	73	2C	69	6E	66
6F	20	30	30	3A	41	41	3A	41	42	3A	30	30	3A	31	46
3A	32	38	40	6F	6C	65	73	7A	2D	61	70	33	3A	20	64
69	73	63	6F	6E	6E	65	63	74	65	64	2C	20	72	65	63
73	61	73	73	6F	63	3A	20	73	61	73	73	6F	63	3A	20
28	38	29	20	0A	6E	6F	76	62	3A	30	30	20	77	69	72
62	75	67	20	6F	6C	65	73	68	3A	32	31	3A	39	35	3A

nov/ 7/2017 23:41:10 by Router OS 6.40.4.# software id = JZXZ-2
GID.#.nov/04 15:51:29 wireless,info 88:83:22:39: A8:BE@olesz-ap3: disconnected, extensive data loss .nov/04 15:51:36 wireless,info 00:AA:AB:00:1F:28@olesz-ap3: disconnected, received disassoc: sending station leaving (8) .nov/04 15:52:00 wireless,debug olesz-ap3: 18:21:95:

Zawartość obiektu

Case Navigator Hex viewer

Hex view Bitmap view Structure view Records view Save all Save selected Extract selected to workspace

from ☒ begin ☐ end (back) ☐ current ☐ current (back)

Go to

Page size Block size User size

Navigation group: None

☐ Use cycle address ☐ Use equal selection

Enter find value

☐ Hex ☐ By offset 0 of 512 bytes block

Find previous Find next Find

Phy image Chip0_0_0 X Workspace

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
☒	0xC0	File header (0x10)	0x0001FD	0x000107	0x00039627	0x0000	0x107	Oleszna_ap3_ap4.log.txt	0x81A4	0x0	0x0	0x58201F7E	0x5A023686	0x5A023686	0x0
☒	0xC0	File header (0x10)	0x0001FD	0x000107	0x00039B1F	0x0000	0x107	Oleszna_ap3_ap4.log.txt	0x81A4	0x0	0x0	0x58201F7E	0x5A062B06	0x5A062B06	0x0
☒	0xC0	File header (0x10)	0x0001FD	0x000107	0x0003A017	0x0000	0x107	Oleszna_ap3_ap4.log.txt	0x81A4	0x0	0x0	0x58201F7E	0x5A0A1F86	0x5A0A1F86	0x0
☒	0xC0	File header (0x10)	0x0001FD	0x000107	0x0003A50A	0x0000	0x107	Oleszna_ap3_ap4.log.txt	0x81A4	0x0	0x0	0x58201F7E	0x5A0E1406	0x5A0E1406	0x0
☒	0xC0	File header (0x10)	0x0001FD	0x000107	0x0003A9FD	0x0000	0x107	Oleszna_ap3_ap4.log.txt	0x81A4	0x0	0x0	0x58201F7E	0x5A120887	0x5A120887	0x0
☒	0xC0	File header (0x10)	0x0001FD	0x000107	0x0003AE8	0x0000	0x107	Oleszna_ap3_ap4.log.txt	0x81A4	0x0	0x0	0x58201F7E	0x5A15FD05	0x5A15FD05	0x0
☒	0xC0	File header (0x10)	0x0001FD	0x000107	0x0003B3CF	0x0000	0x107	Oleszna_ap3_ap4.log.txt	0x81A4	0x0	0x0	0x58201F7E	0x5A19F186	0x5A19F186	0x0
☒	0xC0	File header (0x10)	0x0001FD	0x000107	0x0003B8B8	0x0000	0x107	Oleszna_ap3_ap4.log.txt	0x81A4	0x0	0x0	0x58201F7E	0x5A1DE606	0x5A1DE606	0x0
☒	0xC0	File header (0x10)	0x0001FD	0x000107	0x0003BD9D	0x0000	0x107	Oleszna_ap3_ap4.log.txt	0x81A4	0x0	0x0	0x58201F7E	0x5A21DA85	0x5A21DA85	0x0
☒	0xC0	File header (0x10)	0x0001FD	0x000107	0x0003C27E	0x0000	0x107	Oleszna_ap3_ap4.log.txt	0x81A4	0x0	0x0	0x58201F7E	0x5A25CF06	0x5A25CF06	0x0
☒	0xC0	File header (0x10)	0x0001FD	0x000107	0x0003C761	0x0000	0x107	Oleszna_ap3_ap4.log.txt	0x81A4	0x0	0x0	0x58201F7E	0x5A29C386	0x5A29C386	0x0
☒	0xC0	File header (0x10)	0x0001FD	0x000107	0x0003CC46	0x0000	0x107	Oleszna_ap3_ap4.log.txt	0x81A4	0x0	0x0	0x58201F7E	0x5A2DB805	0x5A2DB805	0x0
☒	0xC0	File header (0x10)	0x0001FD	0x000107	0x0003D12C	0x0000	0x107	Oleszna_ap3_ap4.log.txt	0x81A4	0x0	0x0	0x58201F7E	0x5A31AC86	0x5A31AC86	0x0
☒	0xC0	File header (0x10)	0x0001FD	0x000107	0x0003D60F	0x0000	0x107	Oleszna_ap3_ap4.log.txt	0x81A4	0x0	0x0	0x58201F7E	0x5A35A106	0x5A35A106	0x0

Phy image Chip0_0_0 X

00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

23 20 6E 6F 76 2F 20 37 2F 32 30 31 37 20 32 33

0000A5FFD0 3A 34 31 3A 31 30 20 62 79 20 52 6F 75 74 65 72

0000A5FFE0 4F 53 20 36 2E 34 30 2E 34 0A 23 20 73 6F 66 74

0000A5FFF0 77 61 72 65 20 69 64 20 3D 20 4A 5A 58 5A 2D 32

0000A60000 47 49 44 0A 23 0A 6E 6F 76 2F 30 34 20 31 35 3A

0000A60010 35 31 3A 32 39 20 77 69 72 65 6C 65 73 73 2C 69

0000A60020 6E 66 6F 20 38 38 3A 38 33 3A 32 32 3A 33 39 3A

0000A60030 41 38 3A 42 45 40 6F 6C 65 73 7A 2D 61 70 33 3A

0000A60040 20 64 69 73 63 6F 6E 6E 65 63 74 65 64 2C 20 65

0000A60050 78 74 65 6E 73 69 76 65 20 64 61 74 61 20 6C 6F

0000A60060 73 73 20 0A 6E 6F 76 2F 30 34 20 31 35 3A 35 31

0000A60070 3A 33 3A 20 77 69 72 65 6C 65 73 73 2C 69 6E 66

0000A60080 6F 6F 30 30 3A 41 41 3A 41 42 3A 30 30 3A 31 46

0000A60090 32 38 40 6F 6C 65 73 7A 2D 61 70 33 3A 20 64

0000A600A0 69 73 63 6F 6E 6E 65 63 74 65 64 2C 20 72 65 63

0000A600B0 65 69 76 65 64 20 64 69 73 61 73 73 6F 63 3A 20

0000A600C0 73 65 6E 64 69 6E 67 20 73 74 61 74 69 6F 6E 20

0000A600D0 6C 65 61 76 69 6E 67 20 28 38 29 20 0A 6E 6F 76

nov/ 7/2017 23:41:10 by RouterOS 6.40.4. # software id = JZXZ-2GID

#

nov/04 15:51:29 wireless,info 88:83:22:39:A8:BE@olesz-ap3: disconnected, extensive data loss

nov/04 15:51:36 wireless,info 00:AA:AB:00:1F:28@olesz-ap3: disconnected, received disassoc: sending station leaving (8)

nov/04 15:52:00 wireless,debug olesz-ap3: 18:21:95:84:25:A7 attempts to associate

nov/04 15:52:00 wireless,debug olesz-ap3: 18:21:95:84:25:A7 not in local ACL, by default accept

nov/04 15:52:00 wireless,info 18:21:95:84:25:A7@olesz-ap3: connected

nov/04 15:52:59 wireless,info 18:21:95:84:25:A7@olesz-ap3: disconnected, received death: sending station leaving (3)

nov/04 15:53:01 wireless,debug olesz-ap3: 18:21:95:84:25:A7 attempts to associate

nov/04 15:53:01 wireless,debug olesz-ap3: 18:21:95:84:25:A7 not in local ACL, by default accept

nov/04 15:53:01 wireless,info 18:21:95:84:25:A7@olesz-ap3: connected

nov/04 15:53:49 wireless,info 18:21:95:84:25:A7@olesz-ap3: disconnected, received death: sending station leaving (3)

nov/04 16:39:43 wireless,debug olesz-ap3: F4:42:8F:97:BE:73 attempts to associate

nov/04 16:39:43 wireless,debug olesz-ap3: F4:42:8F:97:BE:73 not in local ACL, by default accept

nov/04 16:39:43 wireless,info F4:42:8F:97:BE:73@olesz-ap3: connected

nov/04 16:40:48 wireless,info F4:42:8F:97:BE:73@olesz-ap3: disconnected, extensive data loss

nov/04 16:54:16 wireless,debug olesz-ap3: 88:83:22:39:A8:BE attempts to associate

nov/04 16:54:16 wireless,debug olesz-ap3: 88:83:22:39:A8:BE not in local ACL, by default accept

nov/04 16:54:16 wireless,info 88:83:22:39:A8:BE@olesz-ap3: connected

nov/04 16:54:47 wireless,info 88:83:22:39:A8:BE@olesz-ap3: disconnected, received death: sending station leaving (3)

nov/04 16:54:48 wireless,debug olesz-ap3: 88:83:22:39:A8:BE attempts to associate

nov/04 16:54:48 wireless,debug olesz-ap3: 88:83:22:39:A8:BE not in local ACL, by default accept

nov/04 16:54:48 wireless,info 88:83:22:39:A8:BE@olesz-ap3: connected

nov/04 16:55:15 wireless,info 88:83:22:39:A8:BE@olesz-ap3: dis??

Ln 25, Col 65 100% Windows (CRLF) UTF-8

Case 3 - Podsumowanie

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

The screenshot displays a forensic analysis workspace with two main windows: a file system browser and two Notepad editors showing system logs.

File System Browser (Phy image Chip0_0_0):

Use	Chunk Type	Object Type	Object Id	Chunk Id	Sequence number	Byte count	Parent Object Id	Name	Permissions	UID	GID	atime	mtime	ctime
☒	0x00 Data (0x00)		0x0001FD	0x000016	0x00050AA2	0x0800								
☒	0x00 Data (0x00)		0x0001FD	0x000017	0x00050AA2	0x068B								
☒	0x00 Data (0x00)		0x0001FD	0x000001	0x00050F69	0x0800								

Notepad Windows (System Logs):

Left Notepad:

```
# nov/ 7/2017 23:41:10 by RouterOS 6.40.4
# software id = JZXZ-2GID

#
nov/04 15:51:29 wireless,info 88:83:22:39:A8:BE@olesz-ap3: disconnected, extensive data loss
nov/04 15:51:36 wireless,info 00:AA:AB:00:1F:28@olesz-ap3: disconnected, received disassoc: sending station leaving (8)
nov/04 15:52:00 wireless,debug olesz-ap3: 18:21:95:84:25:A7 attempts to associate
nov/04 15:52:00 wireless,debug olesz-ap3: 18:21:95:84:25:A7 not in local ACL, by default accept
nov/04 15:52:00 wireless,info 18:21:95:84:25:A7@olesz-ap3: connected
nov/04 15:52:59 wireless,info 18:21:95:84:25:A7@olesz-ap3: disconnected, received deauth: sending station leaving (3)
nov/04 15:53:01 wireless,debug olesz-ap3: 18:21:95:84:25:A7 attempts to associate
nov/04 15:53:01 wireless,debug olesz-ap3: 18:21:95:84:25:A7 not in local ACL, by default accept
nov/04 15:53:01 wireless,info 18:21:95:84:25:A7@olesz-ap3: connected
nov/04 15:53:49 wireless,info 18:21:95:84:25:A7@olesz-ap3: disconnected, received deauth: sending station leaving (3)
nov/04 16:39:43 wireless,debug olesz-ap3: F4:42:8F:97:BE:73 attempts to associate
nov/04 16:39:43 wireless,debug olesz-ap3: F4:42:8F:97:BE:73 not in local ACL, by default accept
nov/04 16:39:43 wireless,info F4:42:8F:97:BE:73@olesz-ap3: connected
nov/04 16:40:48 wireless,info F4:42:8F:97:BE:73@olesz-ap3: disconnected, extensive data loss
nov/04 16:54:16 wireless,debug olesz-ap3: 88:83:22:39:A8:BE attempts to associate
nov/04 16:54:16 wireless,debug olesz-ap3: 88:83:22:39:A8:BE not in local ACL, by default accept
nov/04 16:54:16 wireless,info 88:83:22:39:A8:BE@olesz-ap3: connected
nov/04 16:54:47 wireless,info 88:83:22:39:A8:BE@olesz-ap3: disconnected, received deauth: sending station leaving (3)
nov/04 16:54:48 wireless,debug olesz-ap3: 88:83:22:39:A8:BE attempts to associate
nov/04 16:54:48 wireless,info 88:83:22:39:A8:BE@olesz-ap3: connected
nov/04 16:55:15 wireless,info 88:83:22:39:A8:BE@olesz-ap3: disconnected, extensive data loss
nov/04 16:58:45 wireless,debug olesz-ap3: 18:21:95:84:25:A7 attempts to associate
nov/04 16:58:45 wireless,debug olesz-ap3: 18:21:95:84:25:A7 not in local ACL, by default accept
nov/04 16:58:45 wireless,info 18:21:95:84:25:A7@olesz-ap3: connected
nov/04 16:59:16 wireless,info 18:21:95:84:25:A7@olesz-ap3: disconnected, received deauth: sending station leaving (3)
nov/04 16:59:25 wireless,debug olesz-ap3: 18:21:95:84:25:A7 attempts to associate
nov/04 16:59:25 wireless,debug olesz-ap3: 18:21:95:84:25:A7 not in local ACL, by default accept
nov/04 16:59:25 wireless,info 18:21:95:84:25:A7@olesz-ap3: connected
nov/04 16:59:55 wireless,info 18:21:95:84:25:A7@olesz-ap3: disconnected, received deauth: sending station leaving (3)
```

Right Notepad:

```
# jun/26/2018 5: 0:15 by RouterOS 6.42
# software id = JZXZ-2GID

#
00:00:34 wireless,info 14:5F:94:1F:37:43@olesz-ap3: connected, signal strength -83
00:00:52 wireless,info 14:5F:94:1F:37:43@olesz-ap3: disconnected, received disassoc: sending station leaving (3)
00:00:55 wireless,debug olesz-ap3: 14:5F:94:1F:37:43 attempts to associate
00:00:55 wireless,debug olesz-ap3: 14:5F:94:1F:37:43 not in local ACL, by default accept
00:00:55 wireless,info 14:5F:94:1F:37:43@olesz-ap3: connected, signal strength -83
00:01:13 wireless,info 14:5F:94:1F:37:43@olesz-ap3: disconnected, received disassoc: sending station leaving (3)
00:01:16 wireless,debug olesz-ap3: 14:5F:94:1F:37:43 attempts to associate
00:01:16 wireless,debug olesz-ap3: 14:5F:94:1F:37:43 not in local ACL, by default accept
00:01:16 wireless,info 14:5F:94:1F:37:43@olesz-ap3: connected, signal strength -82
00:01:34 wireless,info 14:5F:94:1F:37:43@olesz-ap3: disconnected, received disassoc: sending station leaving (3)
00:03:52 wireless,debug olesz-ap3: 14:5F:94:1F:37:43 attempts to associate
00:03:52 wireless,debug olesz-ap3: 14:5F:94:1F:37:43 not in local ACL, by default accept
00:03:52 wireless,info 14:5F:94:1F:37:43@olesz-ap3: connected, signal strength -82
00:04:13 wireless,info 14:5F:94:1F:37:43@olesz-ap3: disconnected, received disassoc: sending station leaving (3)
00:04:13 wireless,debug olesz-ap3: 14:5F:94:1F:37:43 attempts to associate
00:04:13 wireless,debug olesz-ap3: 14:5F:94:1F:37:43 not in local ACL, by default accept
00:04:13 wireless,info 14:5F:94:1F:37:43@olesz-ap3: connected, signal strength -84
00:04:31 wireless,info 14:5F:94:1F:37:43@olesz-ap3: disconnected, received disassoc: sending station leaving (3)
00:04:33 wireless,debug olesz-ap3: 14:5F:94:1F:37:43 attempts to associate
00:04:33 wireless,debug olesz-ap3: 14:5F:94:1F:37:43 not in local ACL, by default accept
00:04:33 wireless,info 14:5F:94:1F:37:43@olesz-ap3: connected, signal strength -83
00:04:51 wireless,info 14:5F:94:1F:37:43@olesz-ap3: disconnected, received disassoc: sending station leaving (3)
00:04:54 wireless,debug olesz-ap3: 14:5F:94:1F:37:43 attempts to associate
00:04:54 wireless,debug olesz-ap3: 14:5F:94:1F:37:43 not in local ACL, by default accept
00:04:54 wireless,info 14:5F:94:1F:37:43@olesz-ap3: connected, signal strength -84
00:05:12 wireless,info 14:5F:94:1F:37:43@olesz-ap3: disconnected, received disassoc: sending station leaving (3)
00:05:15 wireless,debug olesz-ap3: 14:5F:94:1F:37:43 attempts to associate
00:05:15 wireless,debug olesz-ap3: 14:5F:94:1F:37:43 not in local ACL, by default accept
00:05:15 wireless,info 14:5F:94:1F:37:43@olesz-ap3: connected, signal strength -81
00:05:33 wireless,info 14:5F:94:1F:37:43@olesz-ap3: disconnected, received disassoc: sending station leaving (3)
00:05:35 wireless,debug olesz-ap3: 14:5F:94:1F:37:43 attempts to associate
00:05:35 wireless,debug olesz-ap3: 14:5F:94:1F:37:43 not in local ACL, by default accept
```

Bottom Panel:

Ln 25, Col 94 | 100% | Windows (CRLF) | UTF-8

Object Id	Chunk Id	Sequence number	Byte count
0x0001FE	0x00000A	0x00047E3A	0x0800
0x0001FE	0x00000B	0x00047E3A	0x0800

Ln 48, Col 27 | 100% | Windows (CRLF) | UTF-8

Object Id	Chunk Id	Sequence number	Byte count
000368A4E0	6C	20 73 74 72 65 6E 67 74 68 20 2D 38 32 20 0A	1 strength -82 .
000368A4F0	30	30 3A 30 31 3A 33 34 20 77 69 72 65 6C 65 73	00:01:34 wireless

Address: 57188736 Selected: 0



Dziękujemy!

www.rusolut.com

Polczyńska 10,

Warsaw, Poland

+48 535 054 431

info@rusolut.com

13-15.06, 2022 Gdynia

