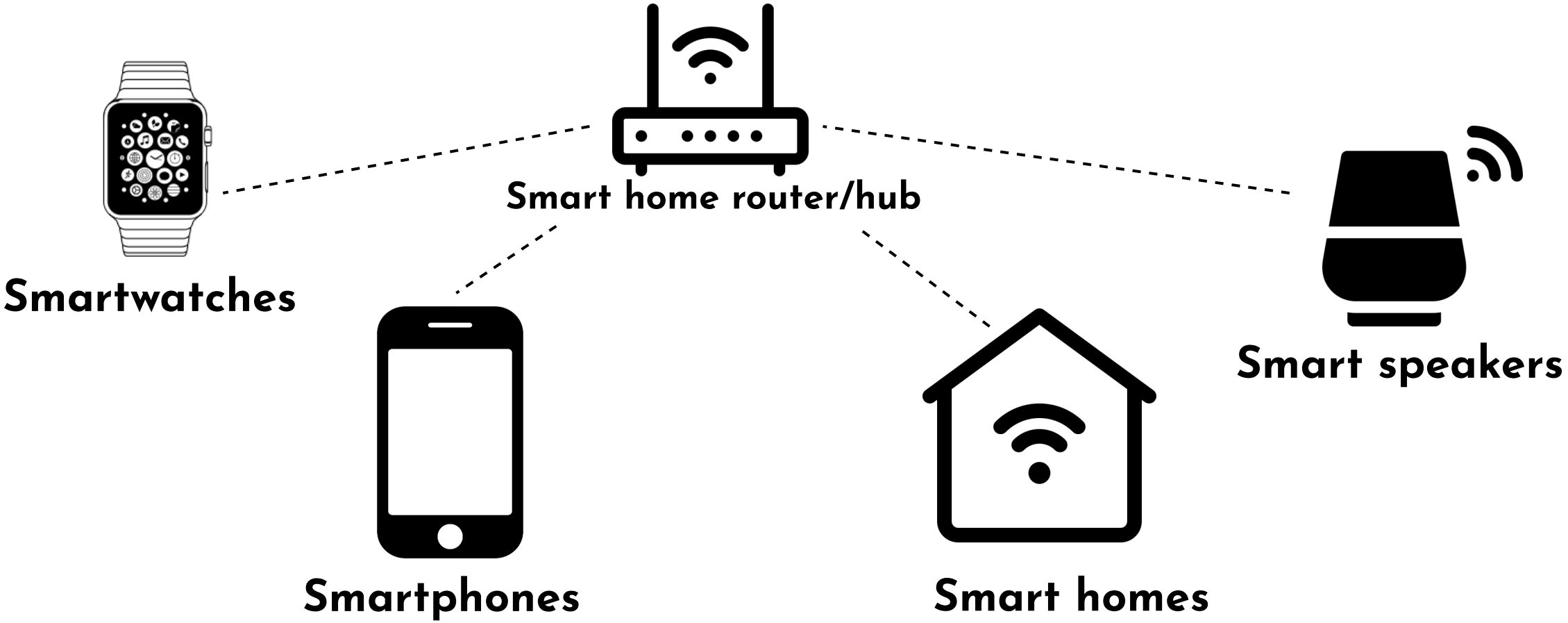
ruSolut

Chip-off Evidence Extraction from IoT Devices

Mykhailo Rybkin - Rusolut

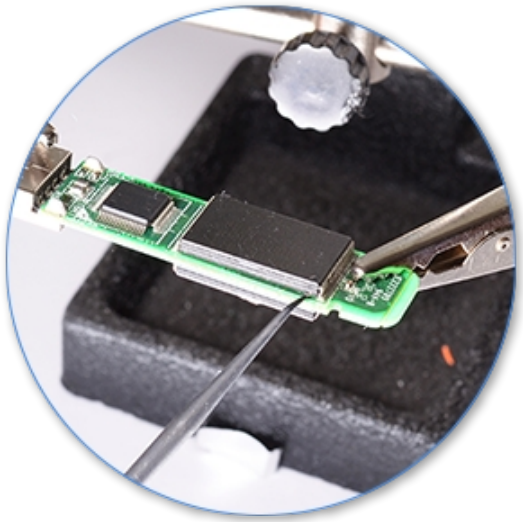
Forensics Europe Expo 2022
8-9 June 2022, London

IoT Network

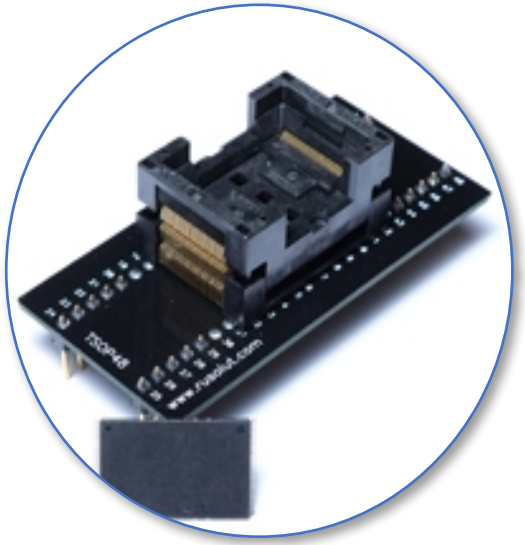

Smart home router/hub
Smartwatches
Smartphones
Smart homes
Smart speakers

Chip-off data recovery method

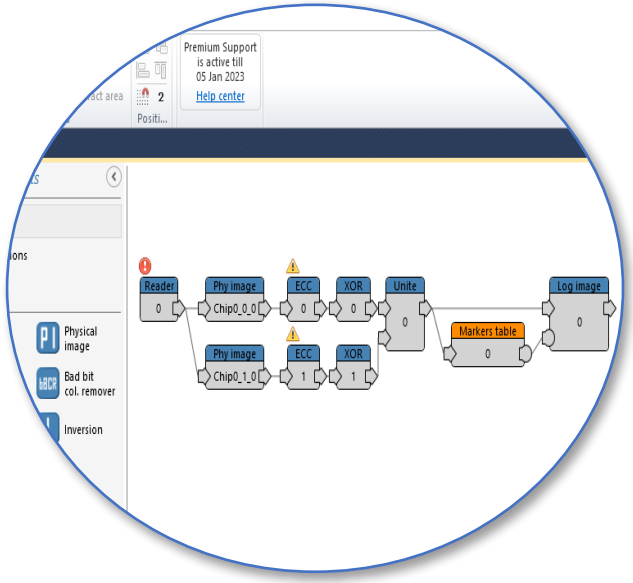
Memory chip unsoldering



Chip identification and adapter selection



Chip reading and file structure re-build



Logical image analysis and file extraction

Chip-off data recovery method advantages

- No risk of overwriting data and losing device logs
- Access to data ensured by password
- Access to all data stored on the device
- Ability to recover data from damaged devices
- Access to deleted via standard interface data

Embedded flash file systems of devices IoT
YAFFS, UBI FS, NAND FS, RAW

Functions

- NAND memory blocks usage optimization (Wear levelling)
- Translation of a physical image into a logical form
- Refresh operations for data allocated in blocks

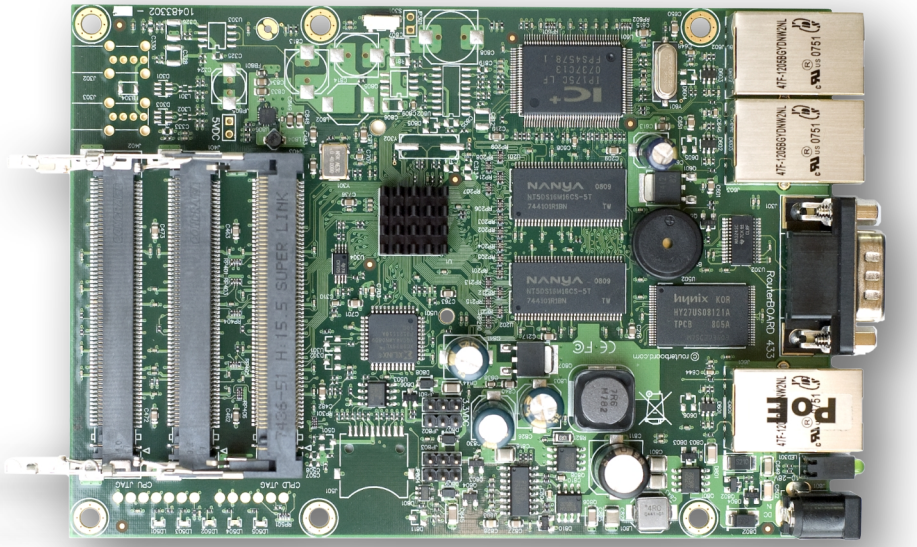
Properties

- No standardized metadata
- Multiple versions of filesystems
- Ability to recover old/deleted data

Case studies

CALIX 844E-1 Wi-Fi Router

Mikrotik RB433GL Wi-Fi Router

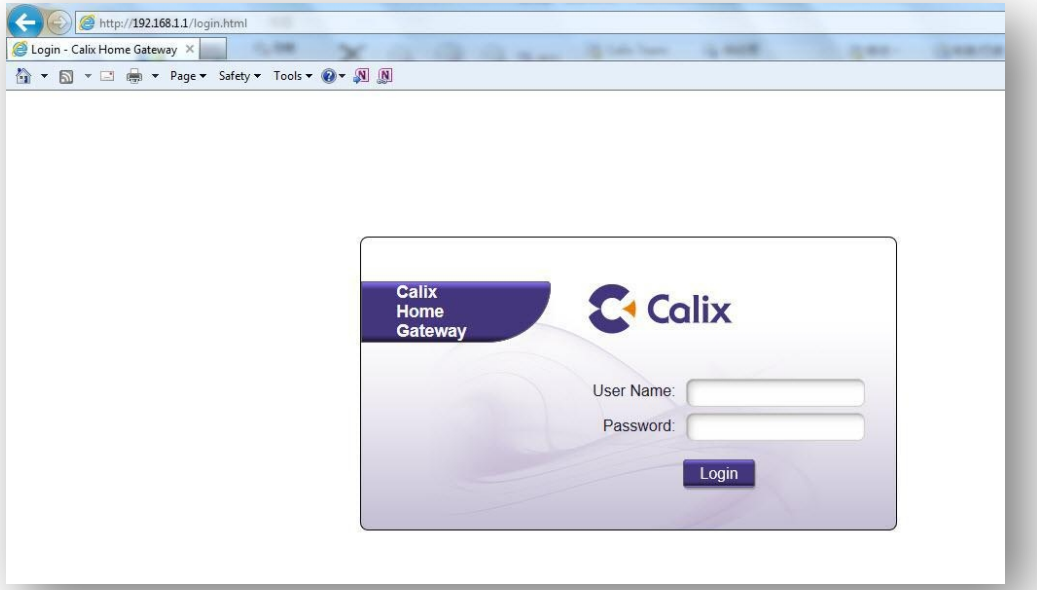


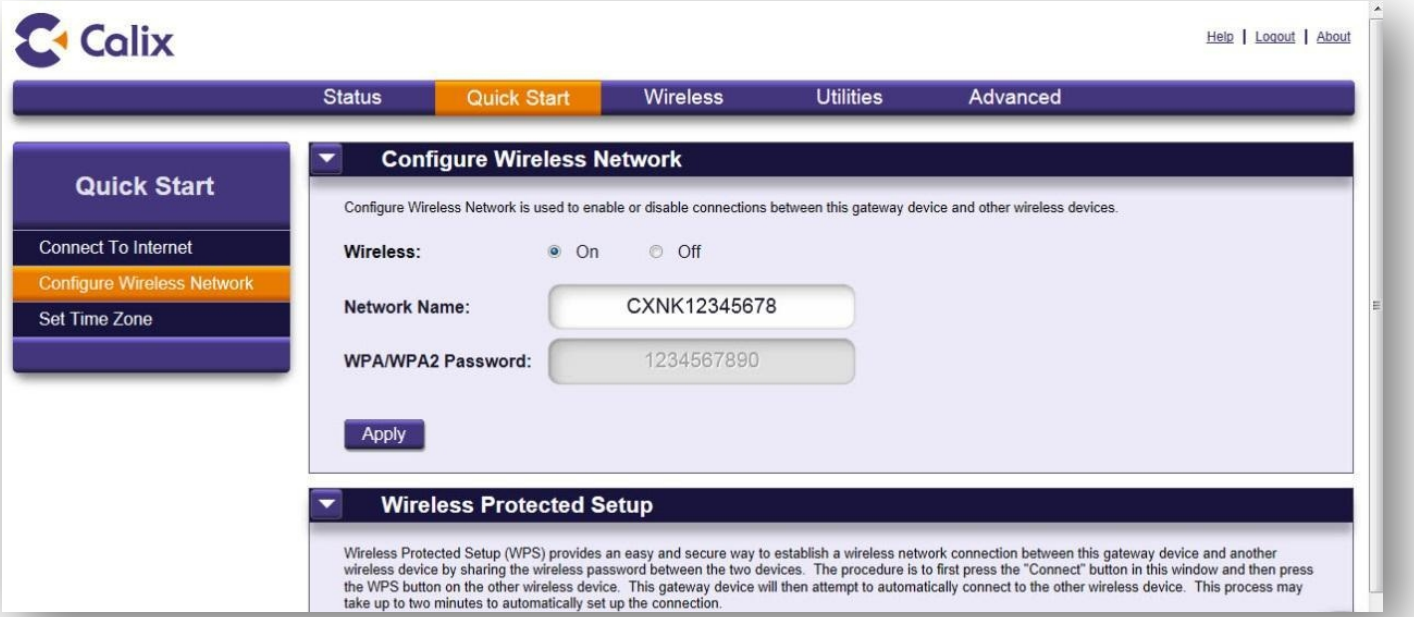
Google Home Speaker

Case 1 - CALIX 844E-1

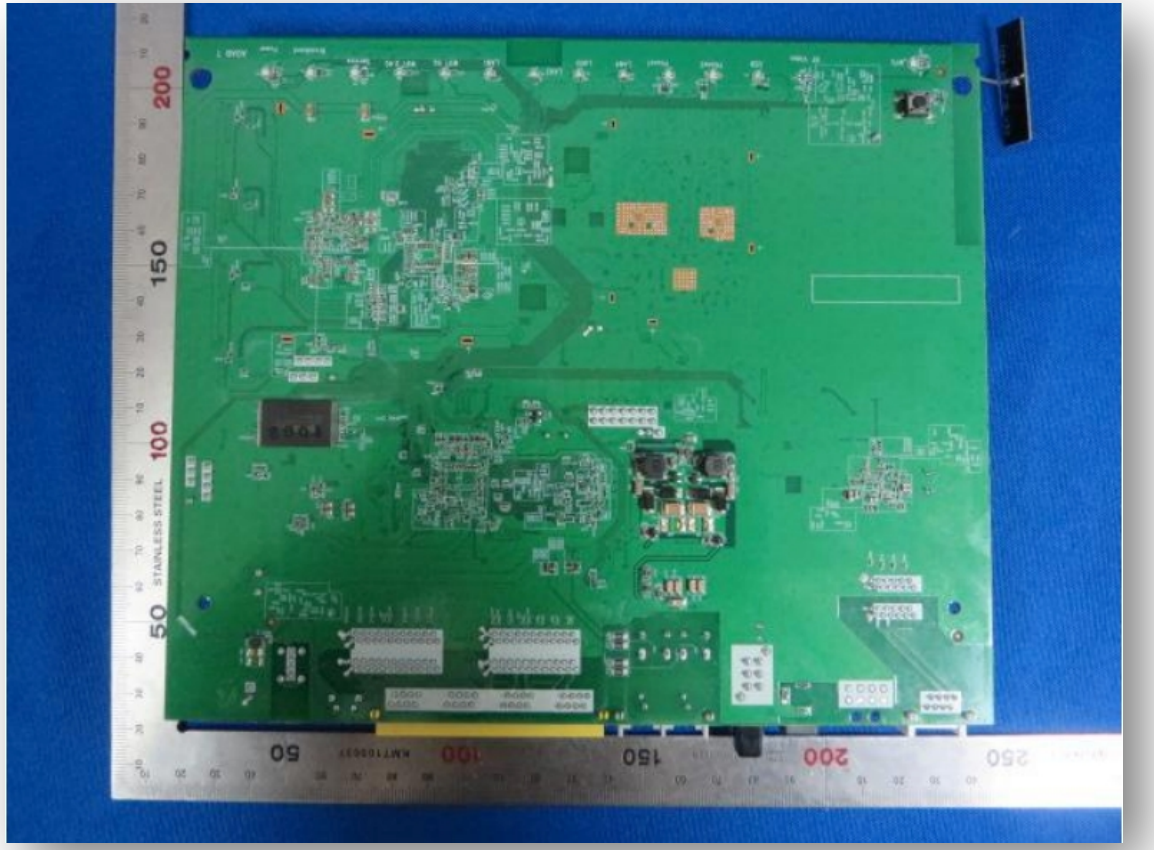
CALIX 844E-1

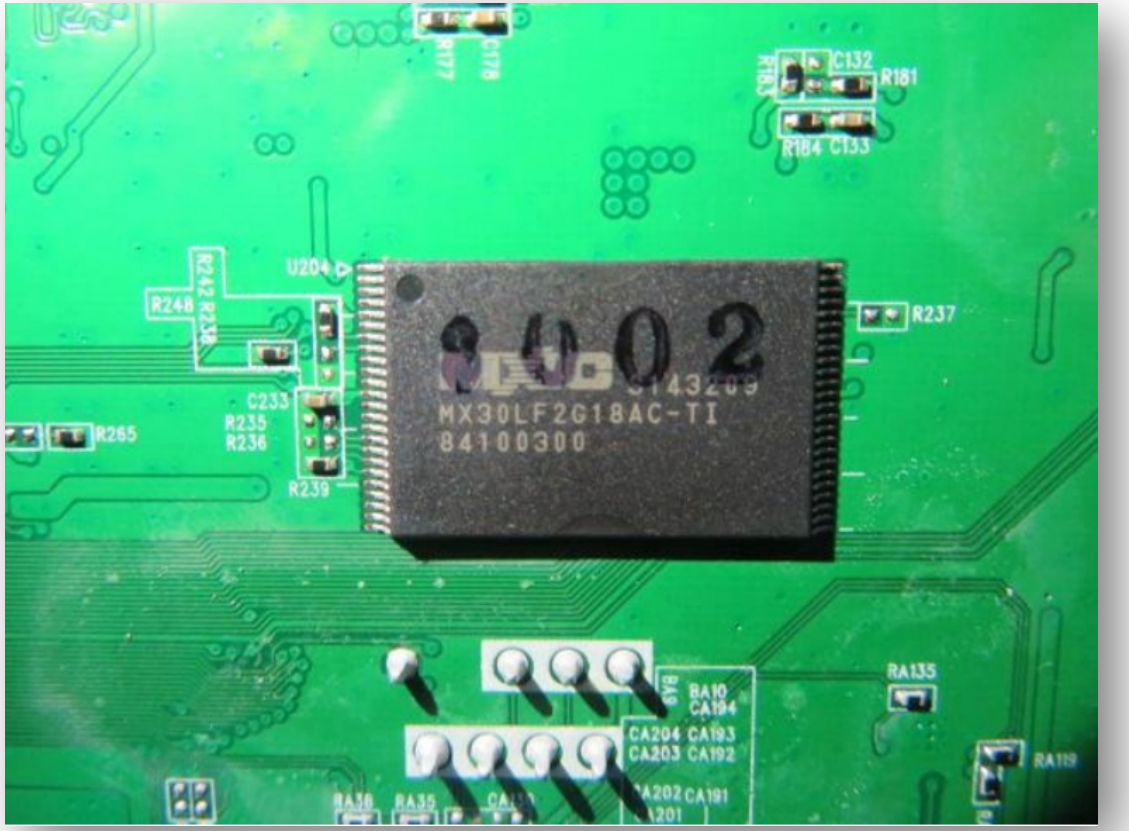
Network software



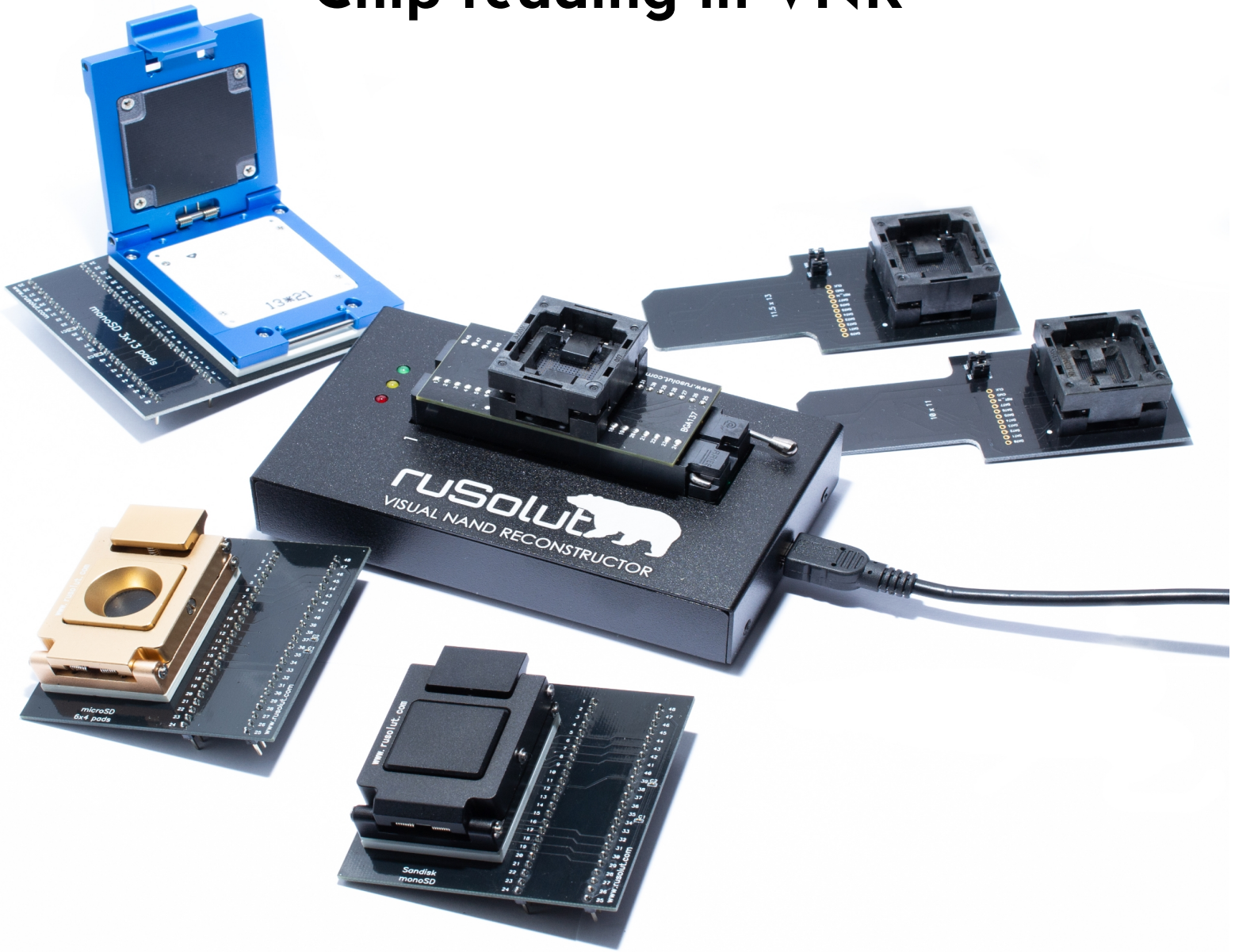


PCB of CALIX 844E-1

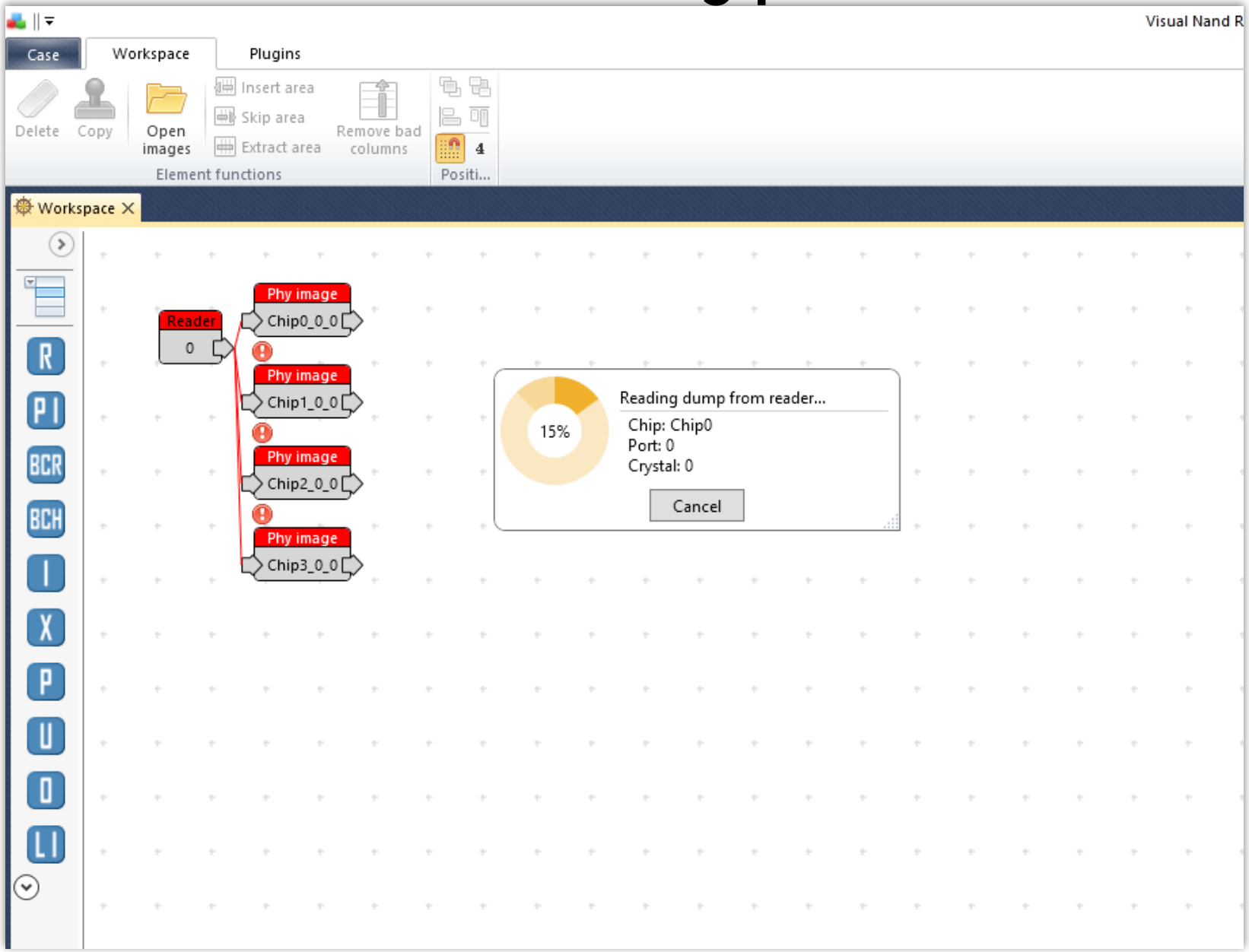




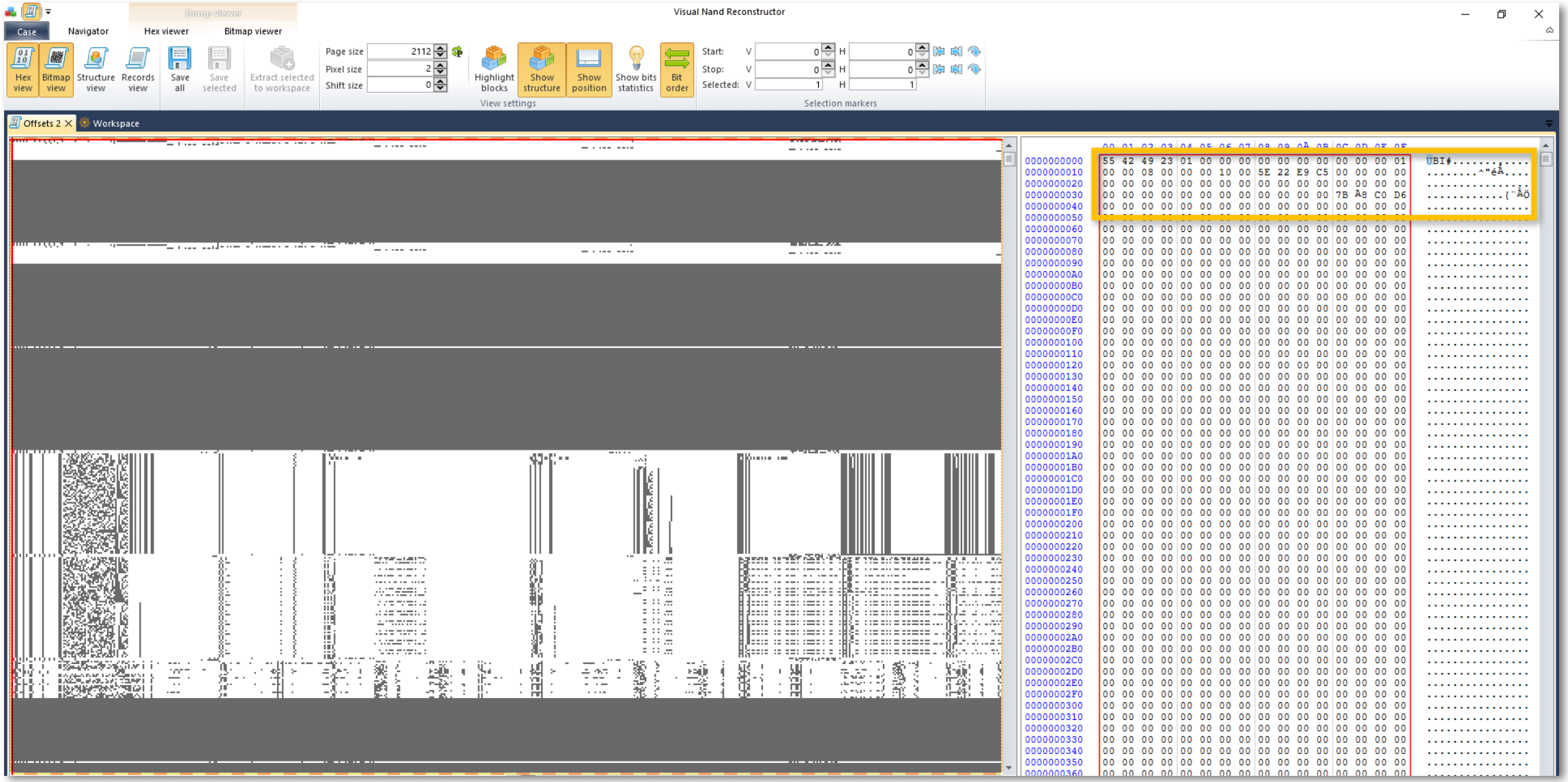
Chip reading in VNR



NAND reading process



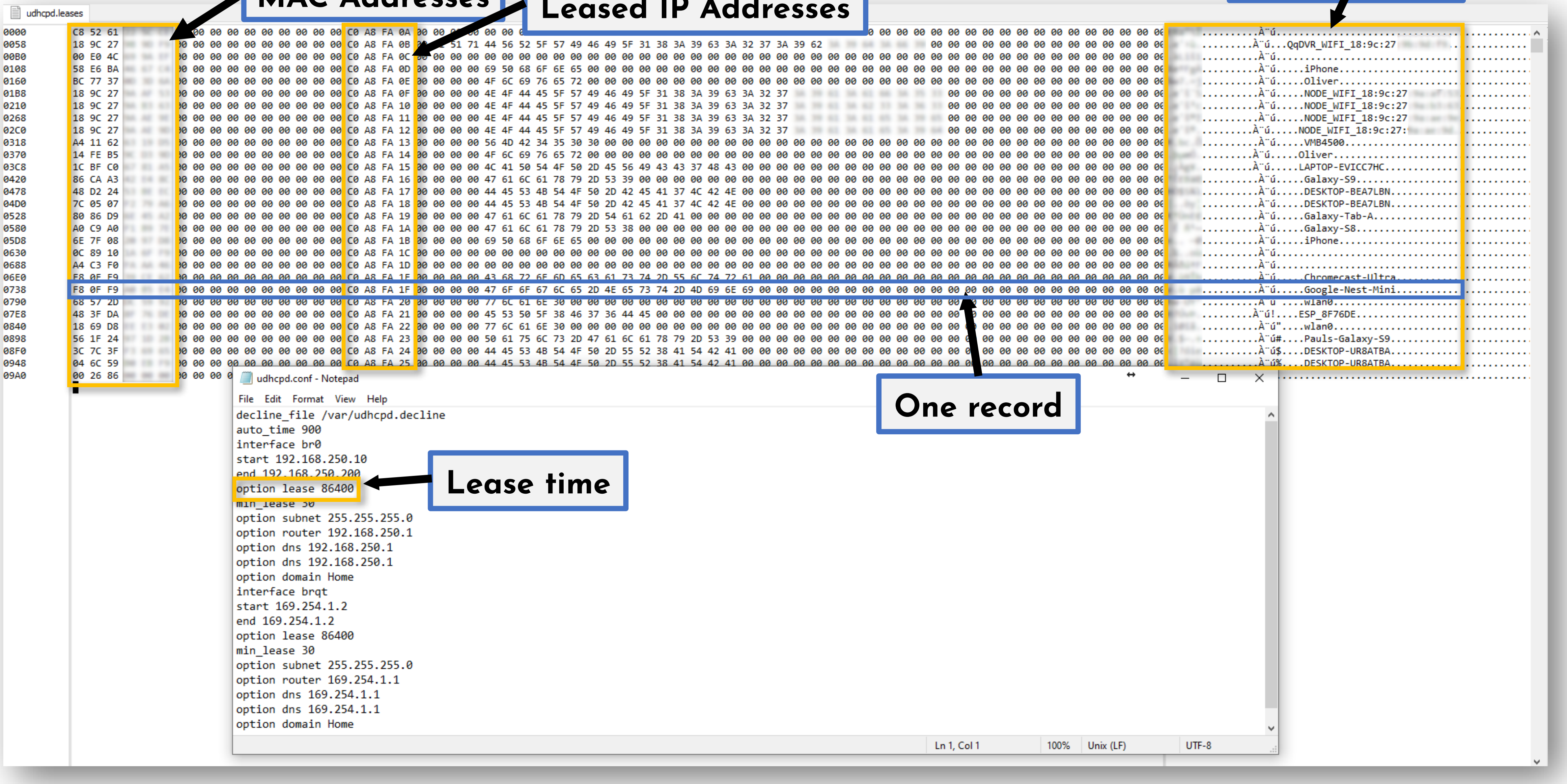
Physical image from NAND chip



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

DHCP Leases



```
0000    C8 52 61 [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 0A 00 00 [illegible] 00 00 00 [illegible] 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  [redacted]..........À¨ú.............................................
0058    18 9C 27 [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 0B [illegible] [illegible] 51 71 44 56 52 5F 57 49 46 49 5F 31 38 3A 39 63 3A 32 37 3A 39 62 [redacted] 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  [redacted].........À¨ú...QqDVR_WIFI_18:9c:27[redacted].................
00B0    00 E0 4C [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 0C 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  [redacted]..........À¨ú.............................................
0108    58 E6 BA [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 0D 00 00 00 00 69 50 68 6F 6E 65 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  [redacted]..........À¨ú.....iPhone..................................
0160    BC 77 37 [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 0E 00 00 00 00 4F 6C 69 76 65 72 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  [redacted]..........À¨ú.....Oliver..................................
01B8    18 9C 27 [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 0F 00 00 00 00 4E 4F 44 45 5F 57 49 46 49 5F 31 38 3A 39 63 3A 32 37 [redacted] 00 00 00 00 00 00 00 00 00 00 00 00 00  [redacted]..........À¨ú.....NODE_WIFI_18:9c:27[redacted].............
0210    18 9C 27 [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 10 00 00 00 00 4E 4F 44 45 5F 57 49 46 49 5F 31 38 3A 39 63 3A 32 37 [redacted] 00 00 00 00 00 00 00 00 00 00 00 00 00  [redacted]..........À¨ú.....NODE_WIFI_18:9c:27[redacted].............
0268    18 9C 27 [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 11 00 00 00 00 4E 4F 44 45 5F 57 49 46 49 5F 31 38 3A 39 63 3A 32 37 [redacted] 00 00 00 00 00 00 00 00 00 00 00 00 00  [redacted]..........À¨ú.....NODE_WIFI_18:9c:27[redacted].............
02C0    18 9C 27 [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 12 00 00 00 00 4E 4F 44 45 5F 57 49 46 49 5F 31 38 3A 39 63 3A 32 37 [redacted] 00 00 00 00 00 00 00 00 00 00 00 00 00  [redacted].........À¨ú.....NODE_WIFI_18:9c:27:[redacted].............
0318    A4 11 62 [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 13 00 00 00 00 56 4D 42 34 35 30 30 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  [redacted]..........À¨ú.....VMB4500.................................
0370    14 FE B5 [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 14 00 00 00 00 4F 6C 69 76 65 72 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  [redacted].........À¨ú.....Oliver..................................
03C8    1C BF C0 [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 15 00 00 00 00 4C 41 50 54 4F 50 2D 45 56 49 43 43 37 48 43 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  [redacted].........À¨ú.....LAPTOP-EVICC7HC.........................
0420    86 CA A3 [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 16 00 00 00 00 47 61 6C 61 78 79 2D 53 39 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  [redacted]..........À¨ú.....Galaxy-S9...............................
0478    48 D2 24 [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 17 00 00 00 00 44 45 53 4B 54 4F 50 2D 42 45 41 37 4C 42 4E 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  [redacted]..........À¨ú.....DESKTOP-BEA7LBN.........................
04D0    7C 05 07 [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 18 00 00 00 00 44 45 53 4B 54 4F 50 2D 42 45 41 37 4C 42 4E 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  [redacted]..........À¨ú.....DESKTOP-BEA7LBN.........................
0528    80 86 D9 [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 19 00 00 00 00 47 61 6C 61 78 79 2D 54 61 62 2D 41 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  [redacted]..........À¨ú.....Galaxy-Tab-A............................
0580    A0 C9 A0 [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 1A 00 00 00 00 47 61 6C 61 78 79 2D 53 38 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  [redacted]..........À¨ú.....Galaxy-S8...............................
05D8    6E 7F 08 [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 1B 00 00 00 00 69 50 68 6F 6E 65 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  [redacted]..........À¨ú.....iPhone..................................
0630    0C 89 10 [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 1C 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  [redacted]..........À¨ú.............................................
0688    A4 C3 F0 [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 1D 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  [redacted]..........À¨ú.............................................
06E0    F8 0F F9 [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 1E 00 00 00 00 43 68 72 6F 6D 65 63 61 73 74 2D 55 6C 74 72 61 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  [redacted]..........À¨ú.....Chromecast-Ultra........................
0738    F8 0F F9 [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 1F 00 00 00 00 47 6F 6F 67 6C 65 2D 4E 65 73 74 2D 4D 69 6E 69 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  [redacted]..........À¨ú.....Google-Nest-Mini........................
0790    68 57 2D [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 20 00 00 00 00 77 6C 61 6E 30 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  [redacted]..........À¨ú ....wlan0...................................
07E8    48 3F DA [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 21 00 00 00 00 45 53 50 5F 38 46 37 36 44 45 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  [redacted].........À¨ú!....ESP_8F76DE..............................
0840    18 69 D8 [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 22 00 00 00 00 77 6C 61 6E 30 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  [redacted]..........À¨ú"....wlan0...................................
0898    56 1F 24 [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 23 00 00 00 00 50 61 75 6C 73 2D 47 61 6C 61 78 79 2D 53 39 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  [redacted]..........À¨ú#....Pauls-Galaxy-S9.........................
08F0    3C 7C 3F [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 24 00 00 00 00 44 45 53 4B 54 4F 50 2D 55 52 38 41 54 42 41 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  [redacted]..........À¨ú$....DESKTOP-UR8ATBA.........................
0948    04 6C 59 [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 25 00 00 00 00 44 45 53 4B 54 4F 50 2D 55 52 38 41 54 42 41 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  [redacted]..........À¨ú%....DESKTOP-UR8ATBA.........................
09A0    00 26 86 [redacted] 00 00 00 [illegible]  ............................................
```

```
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 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
```

MAC Addresses

Leased IP Addresses

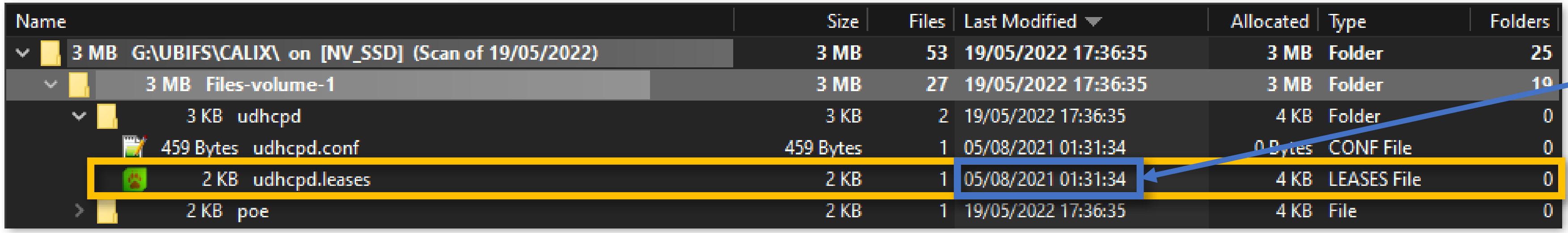
Device name

One record

Lease time

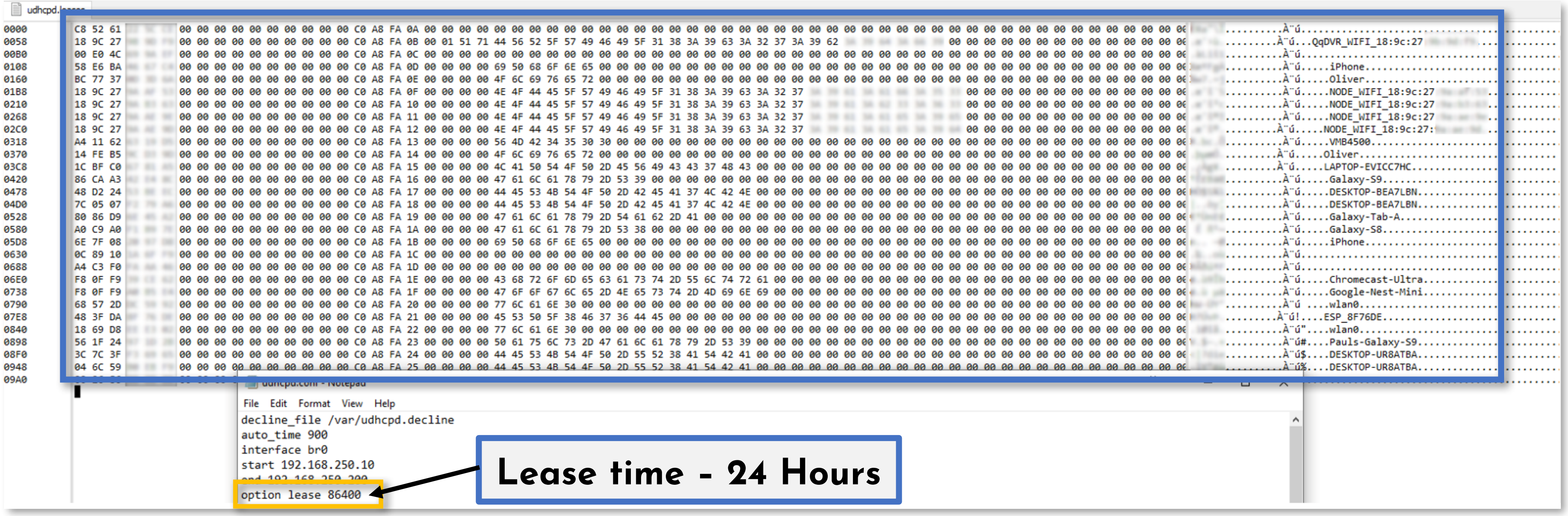
Case 1 - Summary

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



Name	Size	Files	Last Modified	Allocated	Type	Folders
3 MB G:\UBIFS\CALIX\ on [NV_SSD] (Scan of 19/05/2022)	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

05/08/2021 01:31:34
File creation date



```
0000  C8 52 61 [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 0A 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 0 [redacted]..........À¨ú.....................
0058  18 9C 27 [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 0B 00 01 51 71 44 56 52 5F 57 49 46 49 5F 31 38 3A 39 63 3A 32 37 3A 39 62 [redacted] 00 00 00 00 00 00 00 00 00 00 00 00 00 0 [redacted]..........À¨ú...QqDVR_WIFI_18:9c:27[redacted]...
00B0  00 E0 4C [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 0C 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 0 [redacted]..........À¨ú.....................
0108  58 E6 BA [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 0D 00 00 00 00 69 50 68 6F 6E 65 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 0 [redacted]..........À¨ú.....iPhone..........
0160  BC 77 37 [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 0E 00 00 00 00 4F 6C 69 76 65 72 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 0 [redacted]..........À¨ú.....Oliver..........
01B8  18 9C 27 [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 0F 00 00 00 00 4E 4F 44 45 5F 57 49 46 49 5F 31 38 3A 39 63 3A 32 37 [redacted] 00 00 00 00 00 00 00 00 00 00 00 00 0 [redacted]..........À¨ú.....NODE_WIFI_18:9c:27[redacted]..
0210  18 9C 27 [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 10 00 00 00 00 4E 4F 44 45 5F 57 49 46 49 5F 31 38 3A 39 63 3A 32 37 [redacted] 00 00 00 00 00 00 00 00 00 00 00 00 0 [redacted]..........À¨ú.....NODE_WIFI_18:9c:27[redacted]..
0268  18 9C 27 [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 11 00 00 00 00 4E 4F 44 45 5F 57 49 46 49 5F 31 38 3A 39 63 3A 32 37 [redacted] 00 00 00 00 00 00 00 00 00 00 00 00 0 [redacted]..........À¨ú.....NODE_WIFI_18:9c:27[redacted]..
02C0  18 9C 27 [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 12 00 00 00 00 4E 4F 44 45 5F 57 49 46 49 5F 31 38 3A 39 63 3A 32 37 [redacted] 00 00 00 00 00 00 00 00 00 00 00 00 0 [redacted]..........À¨ú.....NODE_WIFI_18:9c:27:[redacted]..
0318  A4 11 62 [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 13 00 00 00 00 56 4D 42 34 35 30 30 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 0 [redacted]..........À¨ú.....VMB4500.........
0370  14 FE B5 [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 14 00 00 00 00 4F 6C 69 76 65 72 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 0 [redacted]..........À¨ú.....Oliver..........
03C8  1C BF C0 [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 15 00 00 00 00 4C 41 50 54 4F 50 2D 45 56 49 43 43 37 48 43 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0 [redacted]..........À¨ú.....LAPTOP-EVICC7HC.........
0420  86 CA A3 [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 16 00 00 00 00 47 61 6C 61 78 79 2D 53 39 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 0 [redacted]..........À¨ú.....Galaxy-S9.........
0478  48 D2 24 [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 17 00 00 00 00 44 45 53 4B 54 4F 50 2D 42 45 41 37 4C 42 4E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0 [redacted]..........À¨ú.....DESKTOP-BEA7LBN.........
04D0  7C 05 07 [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 18 00 00 00 00 44 45 53 4B 54 4F 50 2D 42 45 41 37 4C 42 4E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0 [redacted]..........À¨ú.....DESKTOP-BEA7LBN.........
0528  80 86 D9 [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 19 00 00 00 00 47 61 6C 61 78 79 2D 54 61 62 2D 41 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 0 [redacted]..........À¨ú.....Galaxy-Tab-A.........
0580  A0 C9 A0 [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 1A 00 00 00 00 47 61 6C 61 78 79 2D 53 38 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 0 [redacted]..........À¨ú.....Galaxy-S8.........
05D8  6E 7F 08 [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 1B 00 00 00 00 69 50 68 6F 6E 65 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 0 [redacted]..........À¨ú.....iPhone..........
0630  0C 89 10 [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 1C 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 0 [redacted]..........À¨ú.....................
0688  A4 C3 F0 [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 1D 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 0 [redacted]..........À¨ú.....................
06E0  F8 0F F9 [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 1E 00 00 00 00 43 68 72 6F 6D 65 63 61 73 74 2D 55 6C 74 72 61 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0 [redacted]..........À¨ú.....Chromecast-Ultra.........
0738  F8 0F F9 [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 1F 00 00 00 00 47 6F 6F 67 6C 65 2D 4E 65 73 74 2D 4D 69 6E 69 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0 [redacted]..........À¨ú.....Google-Nest-Mini.........
0790  68 57 2D [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 20 00 00 00 00 77 6C 61 6E 30 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 0 [redacted]..........À¨ú ....wlan0..........
07E8  48 3F DA [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 21 00 00 00 00 45 53 50 5F 38 46 37 36 44 45 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 0 [redacted]..........À¨ú!....ESP_8F76DE.........
0840  18 69 D8 [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 22 00 00 00 00 77 6C 61 6E 30 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 0 [redacted]..........À¨ú"....wlan0..........
0898  56 1F 24 [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 23 00 00 00 00 50 61 75 6C 73 2D 47 61 6C 61 78 79 2D 53 39 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0 [redacted]..........À¨ú#....Pauls-Galaxy-S9.........
08F0  3C 7C 3F [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 24 00 00 00 00 44 45 53 4B 54 4F 50 2D 55 52 38 41 54 42 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0 [redacted]..........À¨ú$....DESKTOP-UR8ATBA.........
0948  04 6C 59 [redacted] 00 00 00 00 00 00 00 00 00 00 C0 A8 FA 25 00 00 00 00 44 45 53 4B 54 4F 50 2D 55 52 38 41 54 42 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0 [redacted]..........À¨ú%....DESKTOP-UR8ATBA.........
09A0
```

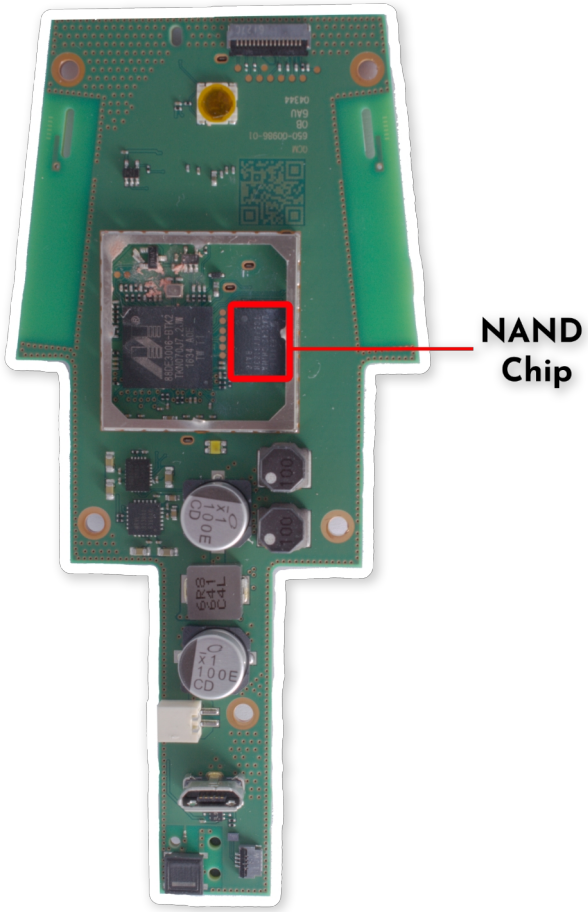
```
decline_file /var/udhcpd.decline
auto_time 900
interface br0
start 192.168.250.10
end 192.168.250.200
option lease 86400
```

Lease time - 24 Hours

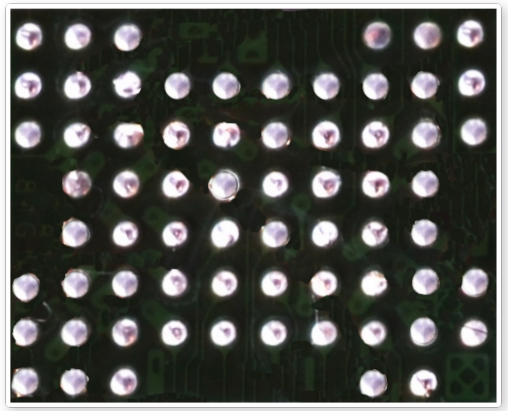
Case 2 - Google Home Speaker

- Fully voice controlled device
- Standard smart speaker functions replicate functions of Google assistant
- Smart home central node
- Compatible with other Chromecast devices

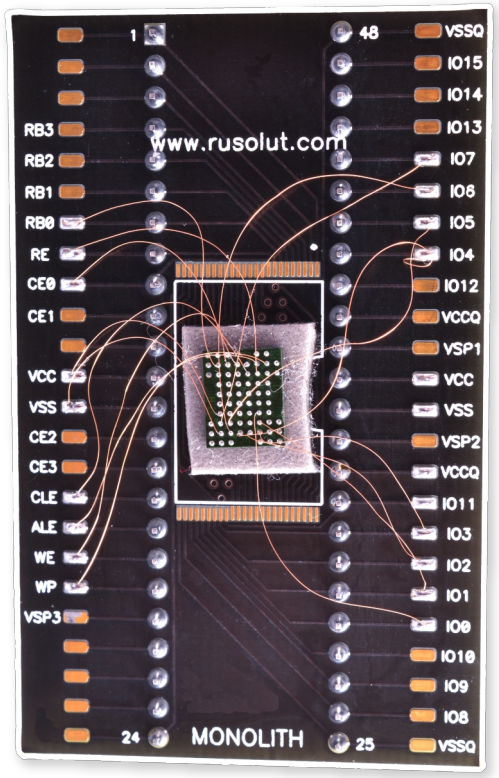
NAND chip extraction and preparations for read-out



Unsoldering

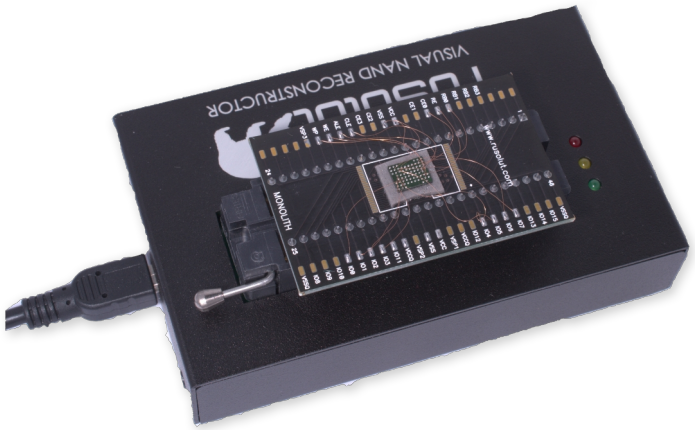


NAND chip

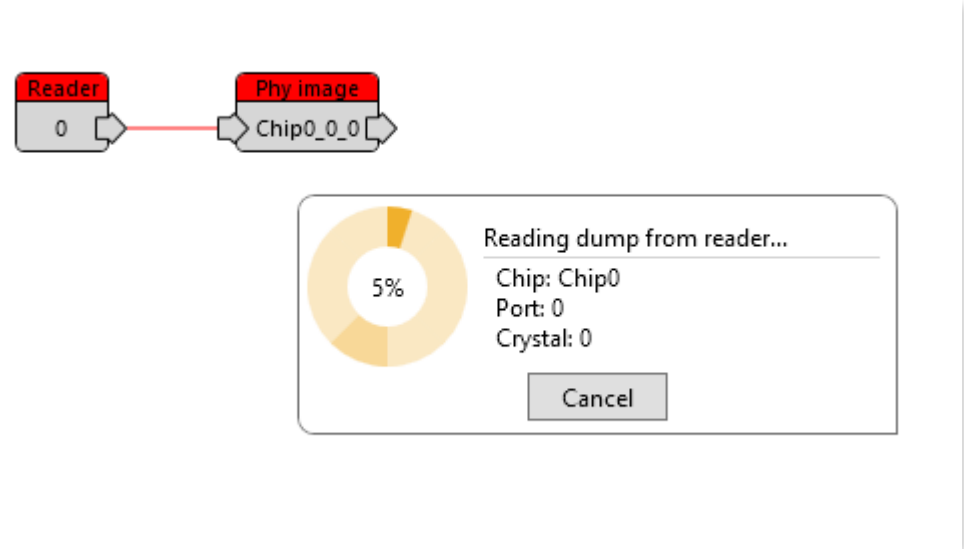


Non-standard package microsoldering

NAND reading process

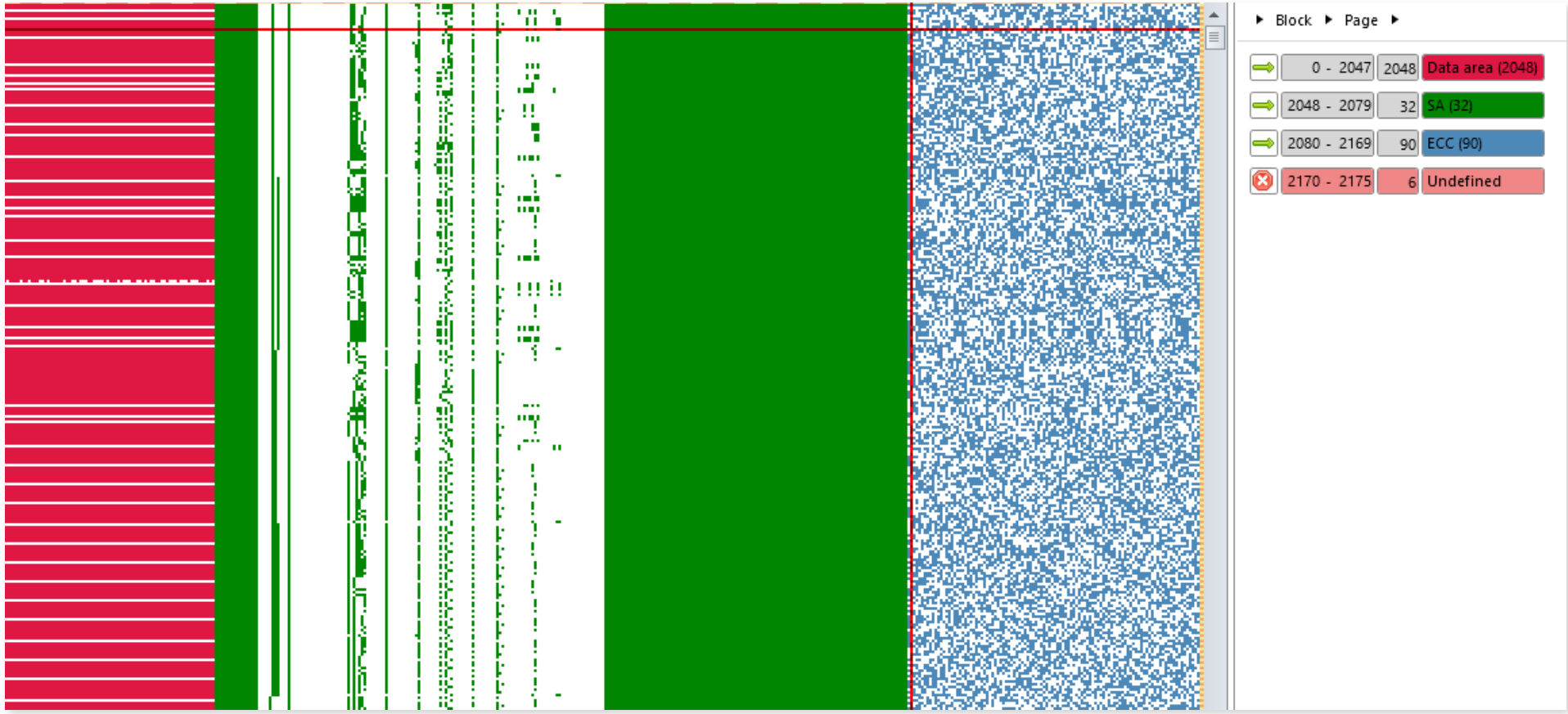


VNR reader with NAND Chip inserted



Software side of reading process

Visual data analysis in VNR



Page structure analysis

First look

Block filter | Block sorter | Meta data offset: 0 | Sequence number offset: 2048 | Object Id offset: 2052 | Chunk Id offset: 2056 | OOB positions | Byte count offset: 2060 | Block status offset | Data status offset | Read OBB | Sync with dump

Offsets 1 | 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

YAFFS parser look in VNR software

Interesting files

Files extracted from researched device #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.

Files extracted from researched device #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.

SSL certificates

client.crt

```
          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

```
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
```

The SSL certificate allows you to decrypt all the traffic of the Smart speaker.
This is where Forensics meets Intelligence… Imagine scenario where you already had traffic collected…

Geo location and client ID

settings

Offsets 0

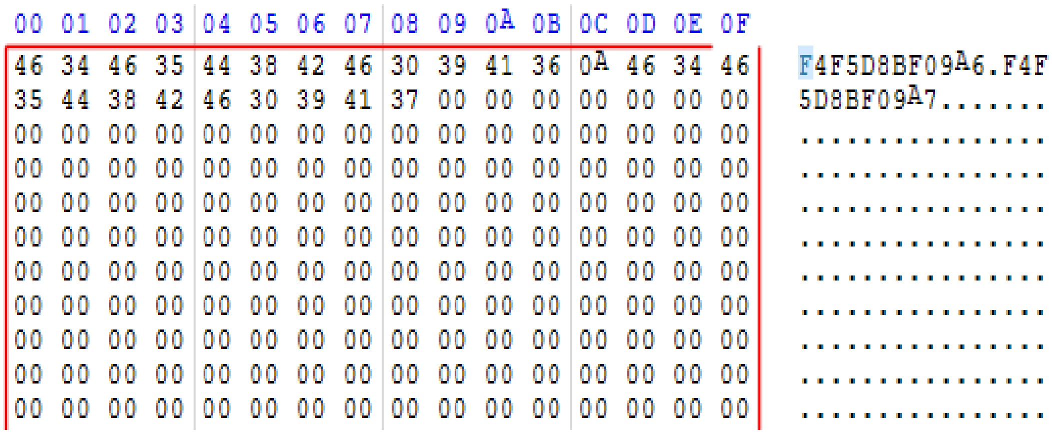
```
          00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
000001DC00 7B 22 67 65 6F 6C 6F 63 61 74 69 6F 6E 22 3A 7B   {"geolocation":{
000001DC10 22 6C 61 74 69 74 75 64 65 22 3A 33 37 2E 33 38   "latitude":37.38
000001DC20 39 34 2C 22 6C 6F 6E 67 69 74 75 64 65 22 3A 2D   94,"longitude":-
000001DC30 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   ................
```

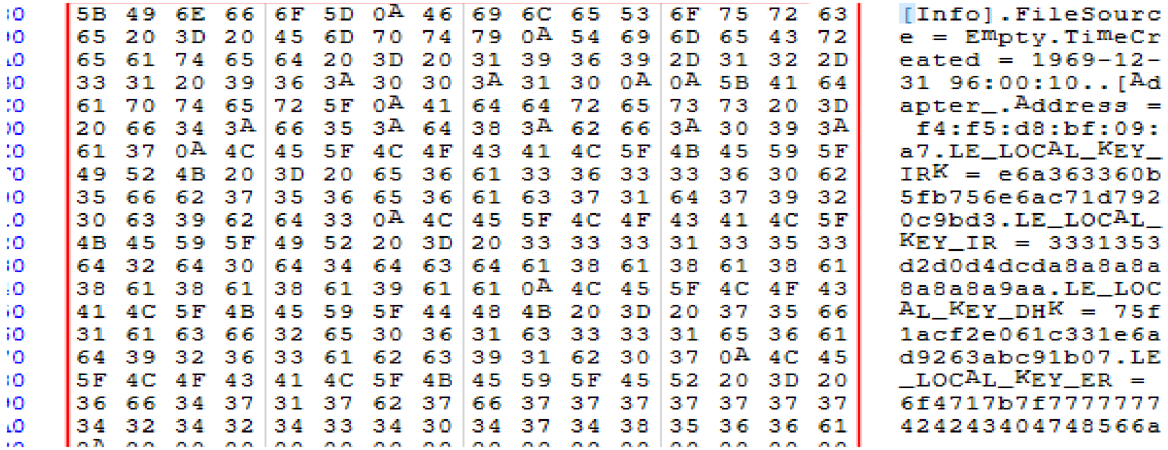
Network config

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



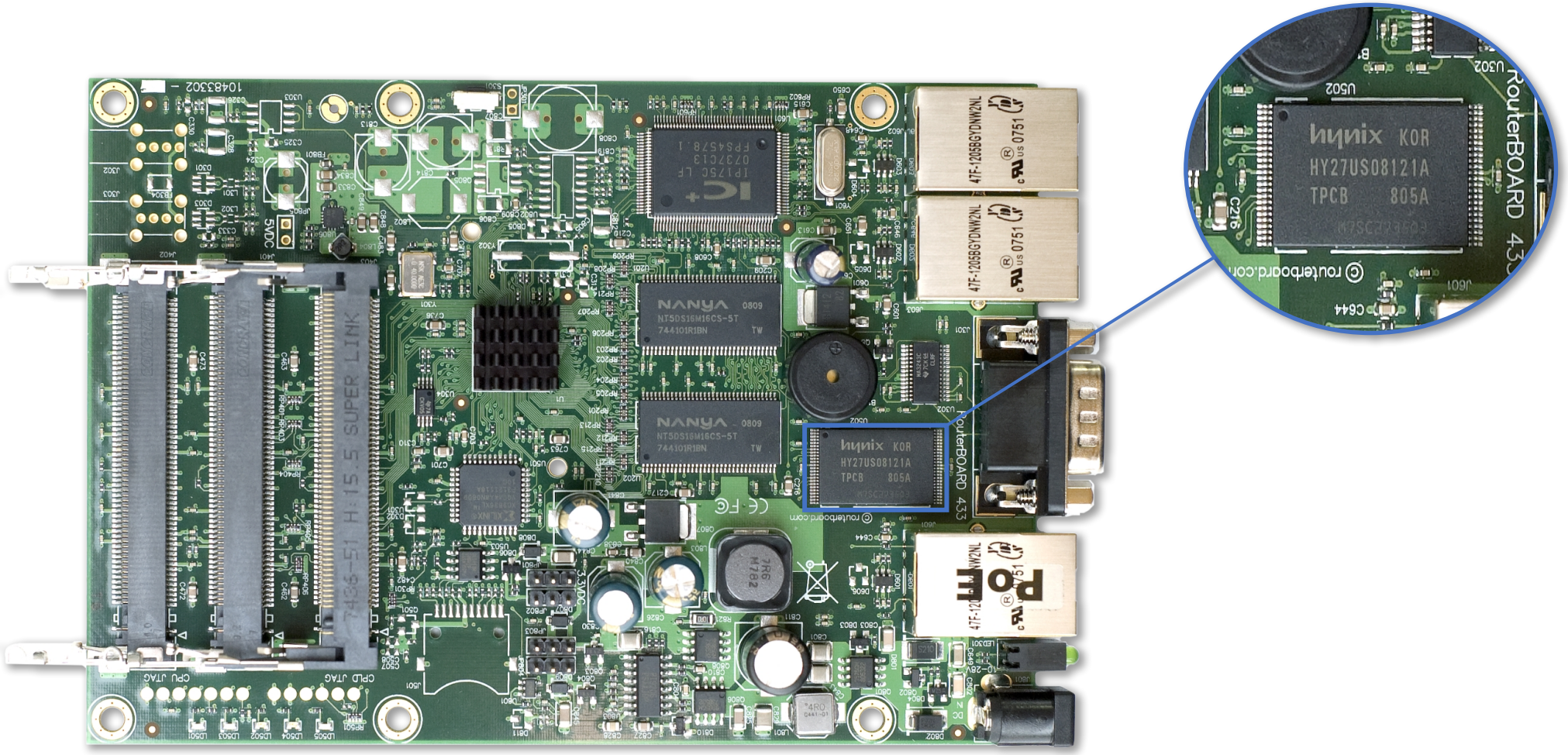
```
5B 49 6E 66 6F 5D 0A 46 69 6C 65 53 6F 75 72 63   [Info].FileSourc
65 20 3D 20 45 6D 70 74 79 0A 54 69 6D 65 43 72   e = Empty.TimeCr
65 61 74 65 64 20 3D 20 31 39 36 39 2D 31 32 2D   eated = 1969-12-
33 31 20 39 36 3A 30 30 3A 31 30 0A 0A 5B 41 64   31 96:00:10..[Ad
61 70 74 65 72 5F 0A 41 64 64 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   424243404748566a
```

Case 2 - Summary

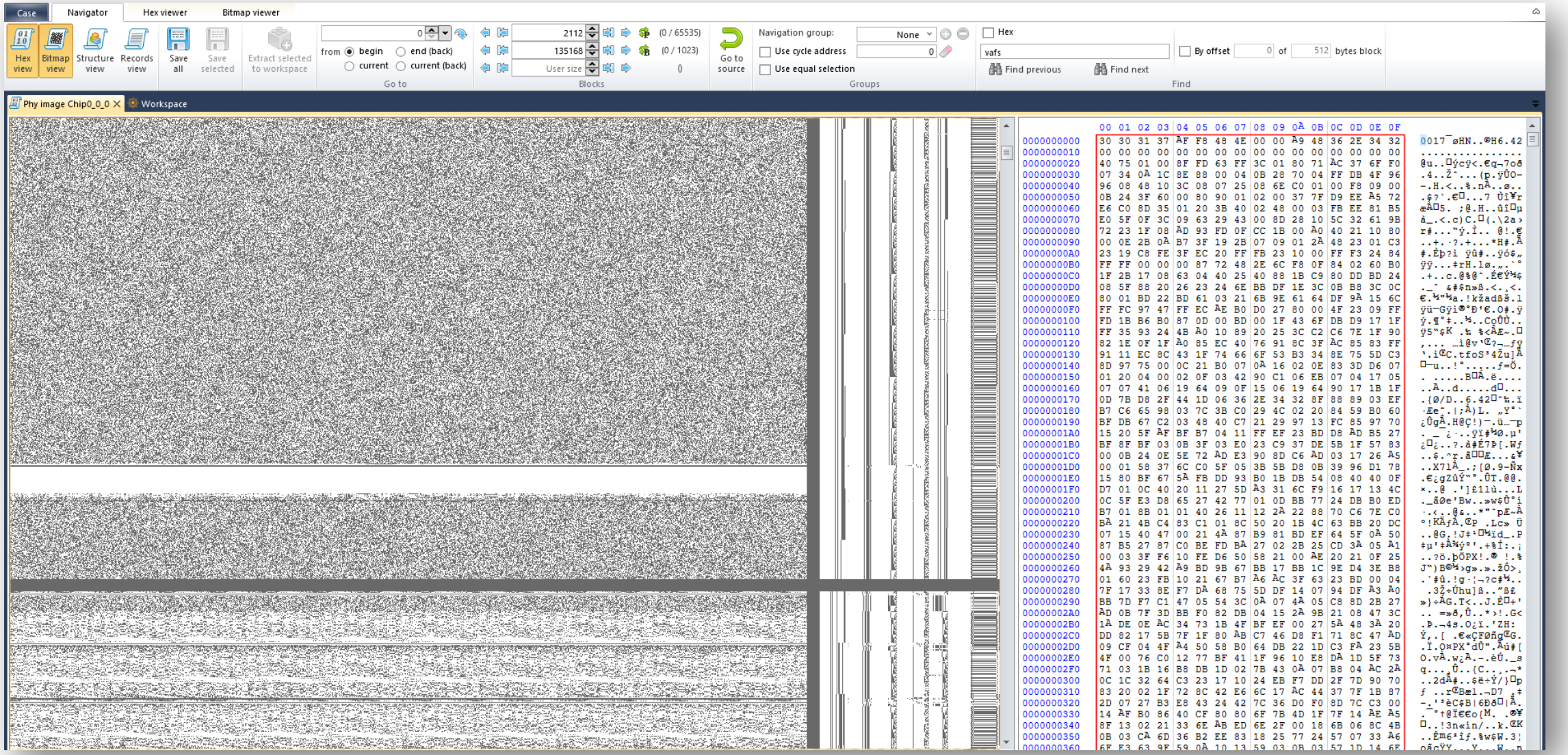
The "first look" into devices shows the “user footprints” are there.
Connecting this information with other parts of puzzle extracted from phone or other evidence may help to piece case together

This research is still ongoing, we are feeding several donor devices with lots of test data in order to pull out more information out of speakers
and understand the whole scale of what is stored there.

Case 3 - Mikrotik RB433GL



YAFFS2 File system



VNR - YAFFS2 parser

Case | Yaffs parser

Block filter | Block sorter | Meta data offset 0 | Sequence number offset 2050 | Object Id offset 2054 | Byte count offset 2062 | Block status offset | Read OBB | Byte order | Sync with dump

File metadata version history

Phy image Chip0_0_0 | 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	0x5A023[illegible]	[illegible]
☑	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

Phy image Chip0_0_0

```
          00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
0000A5FFD0 23 20 6E 6F 76 2F 20 37 2F 32 30 31 37 20 32 33   # nov/ 7/2017 23
0000A5FFE0 3A 34 31 3A 31 30 20 62 79 20 52 6F 75 74 65 72   :41:10 by Router
0000A5FFF0 4F 53 20 36 2E 34 30 2E 34 0A 23 20 73 6F 66 74   OS 6.40.4.# soft
0000A60000 77 61 72 65 20 69 64 20 3D 20 4A 5A 58 5A 2D 32   ware id = JZXZ-2
0000A60010 47 49 44 0A 23 0A 6E 6F 76 2F 30 34 20 31 35 3A   GID.#.nov/04 15:
0000A60020 35 31 3A 32 39 20 77 69 72 65 6C 65 73 73 2C 69   51:29 wireless,i
0000A60030 6E 66 6F 20 38 38 3A 38 33 3A 32 32 3A 33 39 3A   nfo 88:83:22:39:
0000A60040 41 38 3A 42 45 40 6F 6C 65 73 7A 2D 61 70 33 3A   A8:BE@olesz-ap3:
0000A60050 20 64 69 73 63 6F 6E 6E 65 63 74 65 64 2C 20 65    disconnected, e
0000A60060 78 74 65 6E 73 69 76 65 20 64 61 74 61 20 6C 6F   xtensive data lo
0000A60070 73 73 20 0A 6E 6F 76 2F 30 34 20 31 35 3A 35 31   ss .nov/04 15:51
0000A60080 3A 33 36 20 77 69 72 65 6C 65 73 73 2C 69 6E 66   :36 wireless,inf
0000A60090 6F 20 30 30 3A 41 41 3A 41 42 3A 30 30 3A 31 46   o 00:AA:AB:00:1F
0000A600A0 3A 32 38 40 6F 6C 65 73 7A 2D 61 70 33 3A 20 64   :28@olesz-ap3: d
0000A600B0 69 73 63 6F 6E 6E 65 63 74 65 64 2C 20 72 65 63   isconnected, rec
0000A600C0 [illegible] 73 61 73 73 6F 63 3A 20   eived disassoc:
0000A600D0 [illegible] 73 74 61 74 69 6F 6E 20   sending station
0000A600E0 [illegible] 28 38 29 20 0A 6E 6F 76   leaving (8) .nov
0000A600F0 [illegible] 32 3A 30 30 20 77 69 72   /04 15:52:00 wir
0000A60100 [illegible] 62 75 67 20 6F 6C 65 73   eless,debug oles
0000A60110 [illegible] 38 3A 32 31 3A 39 35 3A   z-ap3: 18:21:95:
```

Object content

Case | Navigator | Hex viewer

Hex view | Bitmap view | Structure view | Records view | Save all | Save selected | Extract selected to workspace | Go to source

Go to: from begin / end (back) / current / current (back)

Blocks: Page size / Block size / User size

Groups: Navigation group: None; Use cycle address; Use equal selection

Find: Hex; Enter finding value; Find previous; Find next; By offset 0 of 512 bytes block

Phy image Chip0_0_0 | 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	
☑	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

Phy image Chip0_0_0

```
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
0000A5FFD0  23 20 6E 6F 76 2F 20 37 2F 32 30 31 37 20 32 33   # nov/ 7/2017 23
0000A5FFE0  3A 34 31 3A 31 30 20 62 79 20 52 6F 75 74 65 72   :41:10 by Router
0000A5FFF0  4F 53 20 36 2E 34 30 2E 34 0A 23 20 73 6F 66 74   OS 6.40.4.# soft
0000A60000  77 61 72 65 20 69 64 20 3D 20 4A 58 5A 2D 32 32   ware id = JZXZ-2
0000A60010  47 49 44 0A 23 0A 6E 6F 76 2F 30 34 20 31 35 3A   GID.#.nov/04 15:
0000A60020  35 31 3A 32 39 20 77 69 72 65 6C 65 73 73 2C 69   51:29 wireless,i
0000A60030  6E 66 6F 20 38 38 3A 38 33 3A 32 32 3A 33 39 3A   nfo 88:83:22:39:
0000A60040  41 38 3A 42 45 40 6F 6C 65 73 7A 2D 61 70 33 3A   A8:BE@olesz-ap3:
0000A60050  20 64 69 73 63 6F 6E 6E 65 63 74 65 64 2C 20 65    disconnected, e
0000A60060  78 74 65 6E 73 69 76 65 20 64 61 74 61 20 6C 6F   xtensive data lo
0000A60070  73 73 20 0A 6E 6F 76 2F 30 34 20 31 35 3A 35 31   ss .nov/04 15:51
0000A60080  3A 33 [illegible] 20 77 69 72 65 6C 65 73 73 2C 69 6E 66   :36 wireless,inf
0000A60090  6F [illegible] 30 30 3A 41 41 3A 41 42 3A 30 30 3A 31 46   o 00:AA:AB:00:1F
0000A600A0  [illegible] 32 38 40 6F 6C 65 73 7A 2D 61 70 33 3A 20 64   :28@olesz-ap3: d
0000A600B0  69 73 63 6F 6E 6E 65 63 74 65 64 2C 20 72 65 63   isconnected, rec
0000A600C0  65 69 76 65 64 20 64 69 73 73 61 73 73 6F 63 3A   eived disassoc:
0000A600D0  73 65 6E 64 69 6E 67 20 73 74 61 74 69 6F 6E 20   sending station
0000A600E0  6C 65 61 76 69 6E 67 20 28 38 29 20 0A 6E 6F 76   leaving (8) .nov
0000A600F0  [illegible] 30 20 77 69 72   /04 15:52:00 wir
0000A60100  [illegible] 20 6F 6C 65 73   eless,debug oles
0000A60110  [illegible] 31 3A 39 35 3A   z-ap3: 18:21:95:
0000A60120  [illegible] 74 65 6D 70 74   84:25:A7 attempt
0000A60130  [illegible] 61 74 65 20 0A   s to associate .
0000A60140  [illegible] 32 3A 30 30 20   nov/04 15:52:00
0000A60150  [illegible] 62 75 67 20 6F   wireless,debug o
0000A60160  [illegible] 38 3A 32 31 3A   lesz-ap3: 18:21:
0000A60170  [illegible] 20 6E 6F 74 20   95:84:25:A7 not
0000A60180  [illegible] 4C 2C 20 62 79   in local ACL, by
0000A60190  [illegible] 63 65 70 74 20    default accept
0000A601A0  [illegible] 35 32 3A 30 30   .nov/04 15:52:00
0000A601B0  [illegible] 6E 66 6F 20 31    wireless,info 1
0000A601C0  [illegible] 32 35 3A 41 37   8:21:95:84:25:A7
0000A601D0  [illegible] 20 63 6F 6E 6E   @olesz-ap3: conn
0000A601E0  [illegible] 30 34 20 31 35   ected .nov/04 15
0000A601F0  [illegible] 6C 65 73 73 2C   :52:59 wireless,
0000A60200  [illegible] 39 35 3A 38 34   info 18:21:95:84
0000A60210  [illegible] 7A 2D 61 70 33   :25:A7@olesz-ap3
0000A60220  [illegible] 74 65 64 2C 20   : disconnected,
0000A60230  [illegible] 61 75 74 68 3A   received deauth:
0000A60240  [illegible] 61 74 69 6F 6E    sending station
0000A60250  [illegible] 29 20 0A 6E 6F    leaving (3) .no
0000A60260  [illegible] 30 31 20 77 69   v/04 15:53:01 wi
0000A60270  [illegible] 67 20 6F 6C 65   reless,debug ole
0000A60280  [illegible] 32 31 3A 39 35   sz-ap3: 18:21:95
0000A60290  [illegible] 74 74 65 6D 70   :84:25:A7 attemp
0000A602A0  [illegible] 69 61 74 65 20   ts to associate
0000A602B0  [illegible] 35 33 3A 30 31   .nov/04 15:53:01
0000A602C0  [illegible] 65 62 75 67 20    wireless,debug
0000A602D0  [illegible] 31 38 3A 32 31   olesz-ap3: 18:21
0000A602E0  [illegible] 37 20 6E 6F 74   :95:84:25:A7 not
0000A602F0  [illegible] 43 4C 2C 20 62    in local ACL, b
0000A60300  [illegible] 63 63 65 70 74   y default accept
0000A60310  [illegible] 3A 35 33 3A 30    .nov/04 15:53:0
0000A60320  [illegible] 69 6E 66 6F 20   1 wireless,info
0000A60330  [illegible] 3A 32 35 3A 41   18:21:95:84:25:A
0000A60340  [illegible] 3A 20 63 6F 6E   7@olesz-ap3: con
```

*Untitled - Notepad

File Edit Format View Help

```
# 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,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 - Summary

Obtained access to the full system logs history from the period between 07/11/2018 - 26/06/2018

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								
☑		0x00 Data (0x00)	0x0001FE	0x00000A	0x00047E3A	0x0800								
☑		0x00 Data (0x00)	0x0001FE	0x00000B	0x00047E3A	0x0800								

Phy image Chip0_0_0 | Workspace

```
              00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
000368A180    23 20 6A 75 6E 2F 32 36 2F 32 30 31 38 20 20 35   # jun/26/2018  5
000368A190    3A 20 30 3A 31 35 20 62 79 20 52 6F 75 74 65 72   : 0:15 by Router
000368A1A0    4F 53 20 36 2E 34 32 0A 23 20 73 6F 66 74 77 61   OS 6.42.# softwa
000368A1B0    72 65 20 69 64 20 3D 20 4A 5A 58 5A 2D 32 47 49   re id = JZXZ-2GI
```

*Untitled - Notepad

File Edit Format View Help

```
# 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,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: 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)
```

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

*Untitled - Notepad

File Edit Format View Help

```
# 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
00:04:10 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
```

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

```
000368A4E0    6C 20 73 74 72 65 6E 67 74 68 20 2D 38 32 20 0A   l strength -82 .
000368A4F0    30 30 3A 30 31 3A 33 34 20 77 69 72 65 6C 65 73   00:01:34 wireles
```

Address: 57188736 Selected: 0

VISIT OUR **BOOTH FEE652** TO SEE NEW TOOLS UNVEIL AND TECHNOLOGY IN WORK

THANK YOU

ruSolut

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

June 8-9, 2022 London, UK

CTX
PREVENT • RESPOND • RECOVER
8-9 June 2022
ExCeL London

FORENSICS EUROPE EXPO
8-9 June 2022
ExCeL London