RTX2030

DECT AirSpy

User's Manual

Version: 4.08
JTP 2017.09.08

General

Information contained in this document is subject to change without notice. RTX A/S makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose.

RTX A/S shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishings, performance, or use of this material.

Warranty

This instrument is warranted against defects in material and Workman ship for a period of one year from date of shipment. During the warranty period, RTX A/S will at its option, either repair or replace products, which prove to be defective. For warranty service or repair, this product must be returned to a service facility designated by RTX A/S. Buyer shall prepay shipping charges to RTX A/S and RTX A/S shall pay shipping charges, duties, and taxes for products returned to RTX A/S from another country.

RTX A/S warrants that its software and firmware designated by RTX A/S for use with an instrument will execute its programming instructions when properly installed on that instrument.

RTX A/S does not warrant that the operation of the instrument or firmware will be uninterrupted or error free.

Limitation of Warranty

The foregoing warranty shall not apply to defects resulting from improper or inadequate maintenance by Buyer, Buyer-supplied software or interfacing, unauthorized modification or misuse, operation outside of the environmental specifications for the product, or improper site preparation or maintenance.

NO OTHER WARRANTY IS EXPRESSED OR IMPLIED.

RTX A/S SPECIFICALLY DISCLAIMS THE IMPLIED WARRANTIES OF MERCHANTA-BILITY AND FITNESS FOR A PARTICULAR PURPOSE.

General information

This document and the information contained, is property of RTX A/S, Denmark. Unauthorized copying is not allowed. The information in this document is believed to be correct at the time of writing. RTX A/S reserves the right at any time to change said content, circuitry and specifications.

The general safety precautions, according to the RTX2030 User's Manual, must be observed during all phases of operation. RTX A/S assumes no liability for the customer's failure to comply with these requirements.

The purpose of the document is to provide guidance to users of the RTX2030 DECT AirSpy. The User's manual describes general functions of the tester and describes the use of the Windows® based interface, as well as interfacing with a production application program.

Documentation Information

This User's Manual contains essential items of information needed for general-purpose use of the test equipment.
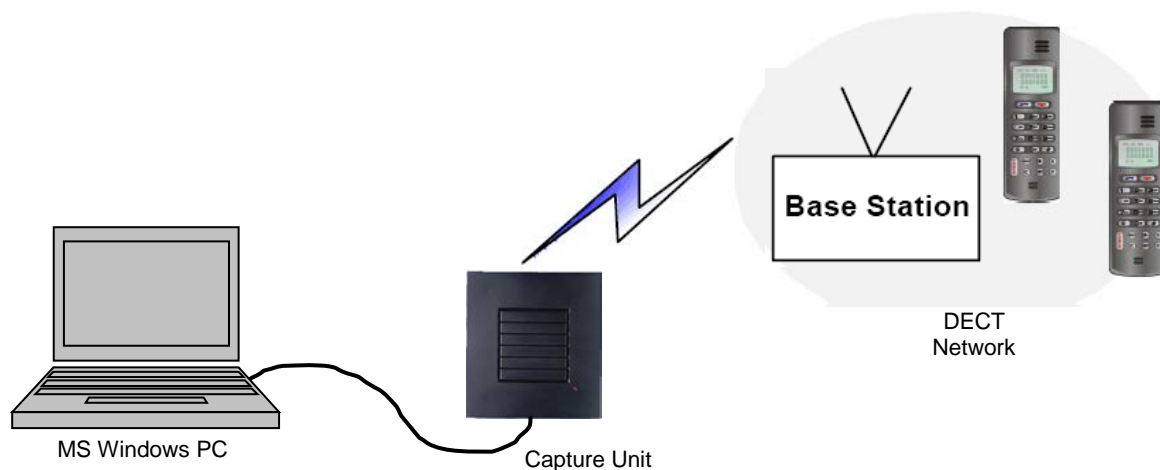
However, please note that the examples and code fragments are included for informational reasons only and should only be used as a guidance to ease test program development. It is therefore strongly emphasized here that RTX A/S takes no responsibility for debugging and verification of the actual test program developed by the customer.

Introduction

The RTX2030 DECT AirSpy tool is a generic DECT communication monitoring and analyzer tool. It can assist product developers and installers with following tasks:
- Protocol analysis
- Deployment analysis in both single and multi-cell environments
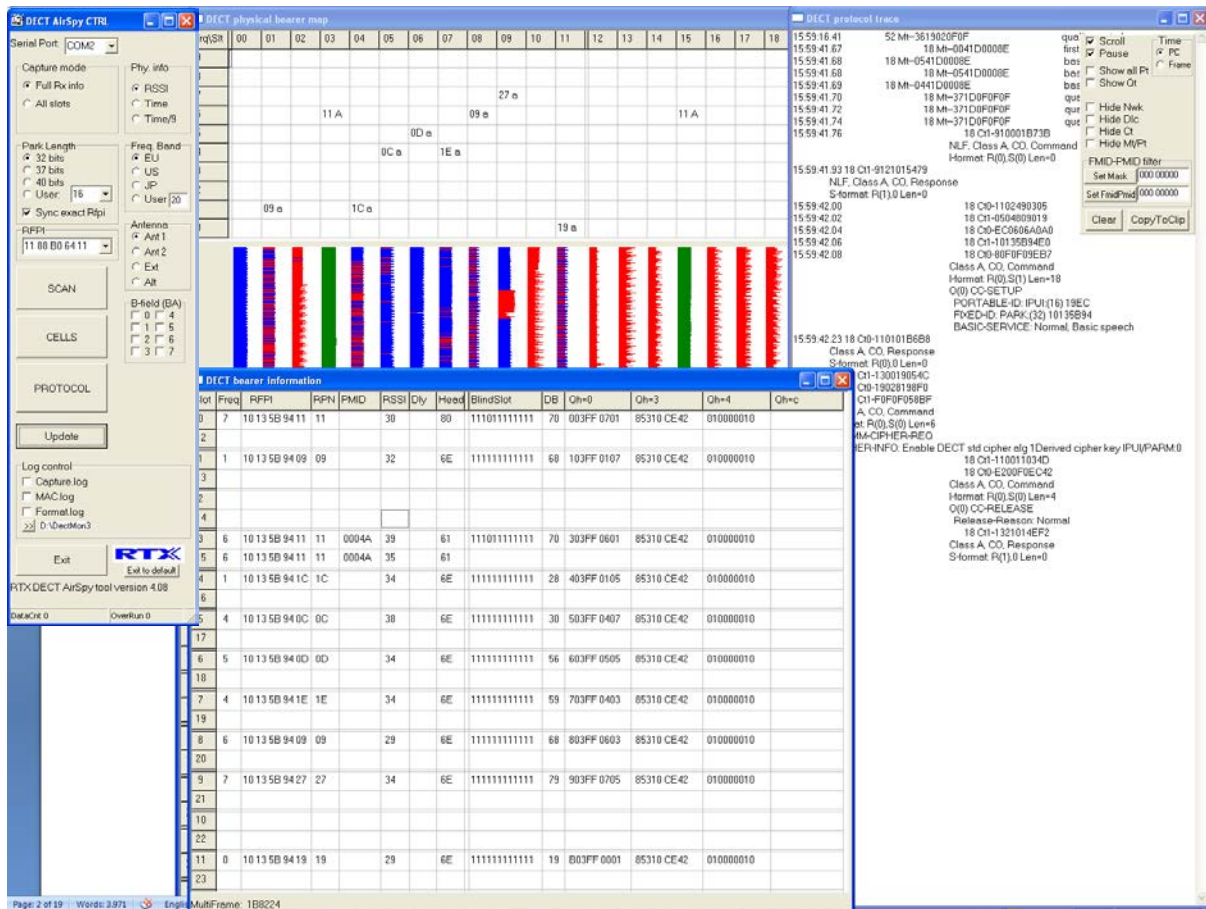- Traffic analysis
- Slot and frame timing analysis

The DECT AirSpy tool consists of a USB powered dedicated DECT RF capture hardware unit and Windows PC applications software. The Capture Unit receives DECT RF signals and performs native packet processing. The collected packets and information are transferred to a PC running Window environment for further analysis and presentation. The Capture Unit can be configured to run in various modes and in selectable frequency bands.

The DECT AirSpy Capture Unit is connected via USB to a standard PC and it receives and decodes the communication between DECT handset and basestations.

The Capture Unit can operate in 3 different modes, optimized for different analysis scenarios:

- Asynchronous slide scanning mode for DECT spectrum discovery.
- Synchronized cell scanning mode for DECT network cell survey and analysis.
- Synchronized bearer receive mode for detailed protocol analysis between FP and PP.

The PC application offers a multi window environment for control and presentation of information from the DECT Capture Unit. The implemented functions and features are:

- Interpretation and display of information on different hierarchical levels:
    - Physical (EU, US and user configurable)
    - MAC (Nt, Pt, Qt and Mt messages)
    - DLC (Class-A messages)
    - NWK
    - Payload (full slot B-field)
- Real-time display of bearer position and physical parameters
- Protocol interpretation
- DECT ULE packet inspection

- Post capture analysis
- Filtering of messages depending on FP and PP identities

- Physical parameter measurements:
    - Signal strength, RSSI
    - Timing analysis with DECT symbol time and 1/9 symbol time resolution

- Generate log files of captured information for further specific analysis

DECT AirSpy detailed description

Table of content:

The following sections is the detailed reference description of the DECT AirSpy features and format of information.

1 Capture Unit

The Capture Unit consists of a DECT RF and baseband electronics able to receive and decode DECT communication. It has built-in antenna and connecter for optional external antenna. It can operate in 3 different capture modes:

- Asynchronous slide scanning mode for spectrum discovery. In this mode it provides spectrum usage overview by measuring RSSI (Signal Strength) and it collects DECT FP information. The Capture Unit is scanning the 10 carriers in the selected band and is sliding by one bit time per frame.

- Synchronized cell scanning mode for DECT network cell survey and analysis. It collects cell usage information such as bearer position and bearer access and HO messages. It performs RSSI and timing measurements on both FP and PP in the network. It is scanning the RF frequencies synchronously with the PSCN. The list of available RF carriers is derived from the FP static system information.

- Synchronized bearer receive mode for detailed protocol analysis of communication between FP and PP. It captures both FP and PP communication in any timeslot. In this mode, the Capture Unit stays locked to a FP network specified by the RFPI/PLI. In idle slots the Capture Unit is scanning the carriers synchronously with the PSCN. In this mode payload in the B-field may be selectively recorded.

The Capture Unit has a LED indicating synchronization state:

- **Flashing**: The Capture Unit is searching for FP with the specified RFPI/PLI. No information a captured.

- **Steady on**: The Capture Unit is synchronized to the FP with the specified RFPI/PLI. Information are being captured and transferred to the PC application.

2 PC application software

The application software installed on a Windows PC is used to configure and control the Capture Unit as well as store, analyze and present data from the Capture Unit. The Capture Unit is connected via a powered USB interface, which offers a virtual serial COM port for transferring data to the PC application.

2.1 Operation mode selection and control

The main modes and operation are controlled from a common control pane, **DECT AirSpy CTRL**. The top part contains various settings to be used by the Capture Unit. The middle part has buttons to select capture mode and the lower part is used to select capture log files.

Capture Unit settings (changes have only effect after any capture mode select).

Capture mode select

Log file operation control

Communication status

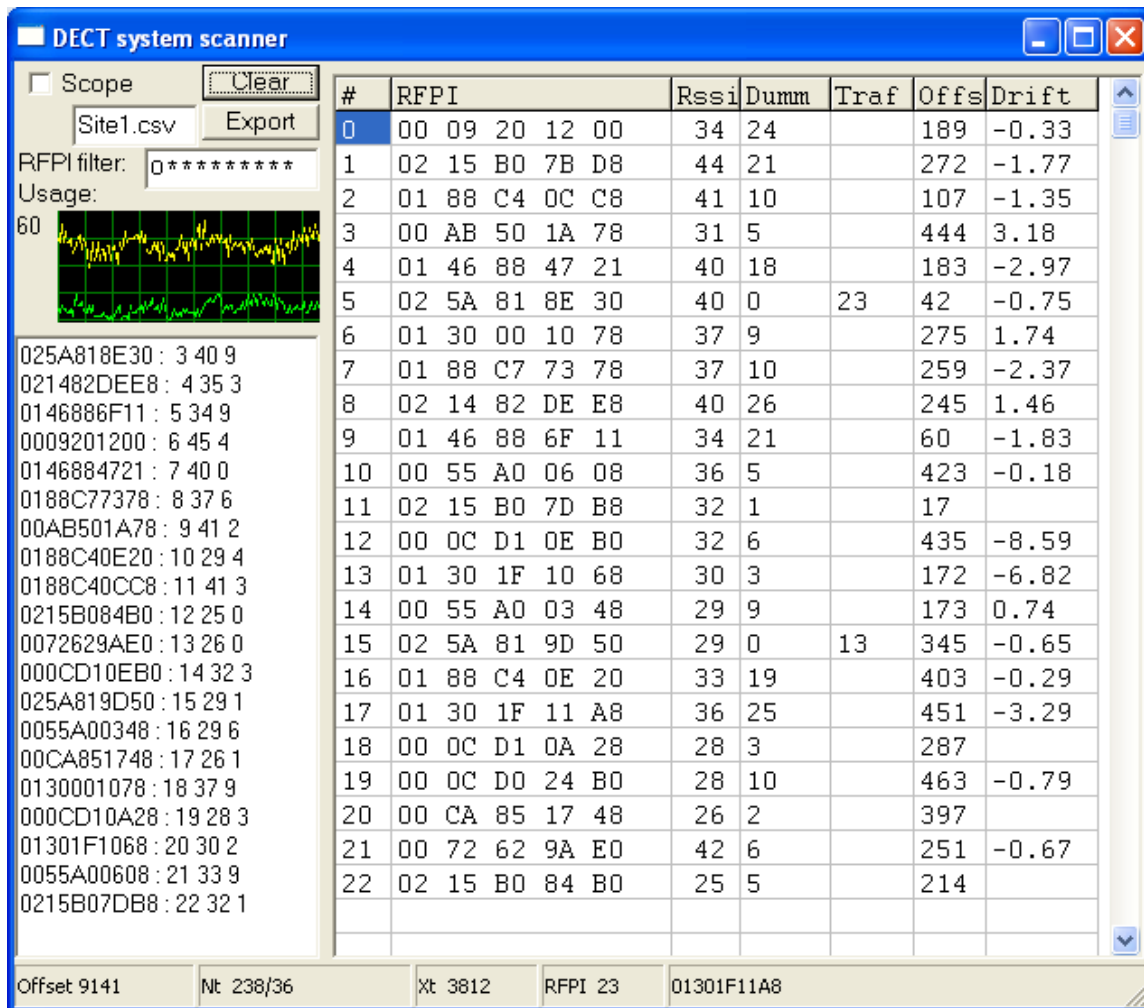| Control	Description
Serial Port:	Communication port to be used for communication with the Capture Unit. The dropdown box will list the available ports.
Full Rx Info	Capture Unit collects every 2nd full slot (12 slots, RSSI and timing)
All slots	Capture Unit collects every A-field (24 slots, RSSI or timing)
RSSI	Capture RSSI in "All slots" mode
Time	Capture DECT bit timing resolution in "All slots" mode
Time/9	Capture DECT 1/9 bit timing resolution in "All slots" mode
Park Length	Specify number of bit match when Capture Unit synchronizes to FP (PLI)
Sync Exact Rfpi	Select if the capture shall only track timing of the specified RFPI
RFPI	FP identity the Capture Unit shall synchronize to
EU	European DECT frequency band: 1880 – 1900MHz
US	US DECT frequency band: 1920 – 1930MHz
JP	Japan DECT frequency band: 1895 - 1902 MHz
User	Define channel offset relative to European DECT channels
	In all frequency bands, extended carrier numbering is supported if transmitted by the basestation
Ant 1	Use internal antenna 1
Ant 2	Use internal antenna 2
Ext	Use external antenna
Alt	Alternate between the two internal antennas
B-field (BA)	Select which B-field content to be captured depending on header field BA value. Is only possible in PROTOCOL capture mode and Full Rx Info.
SCAN	Command the Capture Unit to switch to operate in asynchronous scanning mode.
CELLS	Command the Capture Unit to switch to operate in synchronous cell scanning mode.
PROTOCOL	Command the Capture Unit to switch to operate in synchronous protocol capture mode.
Update	Command the Capture Unit to reload all the settings above.
Capture.log	Produce native binary capture log file. File is open and close when field is checked and unchecked.
MAC.log	Produce MAC log file. File is open and close when field is checked and unchecked.
Format.log	Produce Format log file. File is open and close when field is

	checked and unchecked.
>>	Change directory for log files
Exit	Exit DECT AirSpy application and save current configuration.
Exit to default	Exit DECT AirSpy application and return to default configuration
DataCnt	Display number of data octets transferred from the Capture Unit to PC application. When counting, it indicates the Capture Unit is synchronized and collecting data.
OverRun	Display number times data has been lost in the communication from the Capture Unit to the PC.
MaxQueue	Display maximum number of data octets that has been buffered in the PC application.

2.2 Information displays

Various display panes show information on different levels depending on current capture mode:

Mode	Available information
SCAN	DECT system scanner DECT spectrum map (Scope)
CELLS	DECT physical bearer map DECT cell overview
PROTOCOL	DECT physical bearer map DECT bearer information DECT protocol trace

2.2.1 DECT system scanner

This is the main window when selecting SCAN mode. It is used to discover identity of available networks. In the left part is listed the RFPI as they are detected. Each RFPI is followed by an index number, RSSI level at first detection and the RF carrier number at first detection.

In the right part of the window is built at table of the same RFPI. This table is built with FP with strongest signal first in the list. For each FP information is displayed:

Column	Description
RFPI	FP identity (Radio Fixed Part Identity)
Rssi	Most recent detect signal strength
Dumm	Number of times a dummy bearer slot has been detected.
Traf	Number of times a traffic bearer slot has been detected.
Offs	Most recent bit time offset related to Capture Unit timeslot borders
Drift	Estimated timing drift related to Capture Unit timing reference (ppm)

Use left mouse click to select a RFPI. The selected RFPI is automatically copied in to the RFPI field in *DECT AirSpy CTRL* pane.

The Clear button flushes the list of detected FP. It has no effect to the Capture Unit.

The Scope checkbox enables the DECT spectrum map, see below.

The Export button may be used to export the entire information in scan windows to a CSV file, which be opened and analyzed in MS Excel. The filename is entered in the field left to the button. When exported, this field turns green when successful and red if an error had occurred. In case of error, modify the filename and retry export.

The RFPI filter can be setup to show only specific groups of RFPI values. One or more hexadecimal values can be entered from left. Default value '**********' allows display of all values.

The *Usage* field shows during the asynchronous scanning for basestations the number timeslot pairs that are free and busy.
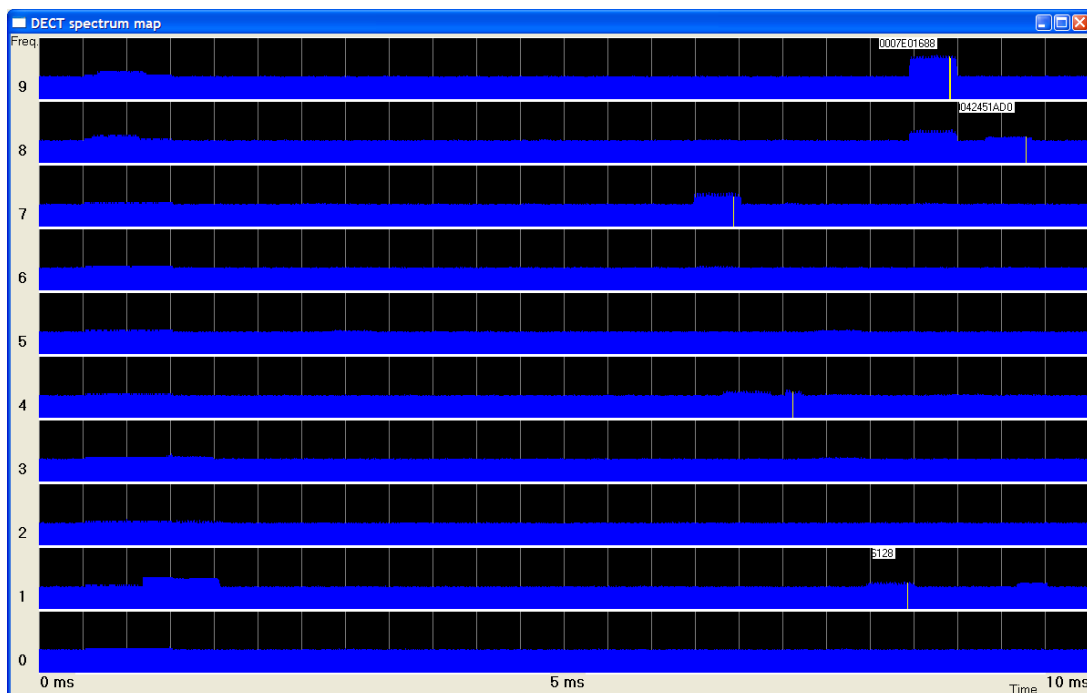Green graph indicates free (=silent) RSSI level of below 32 native level.
Yellow graph indicates busy RSSI level of above 40 native level.
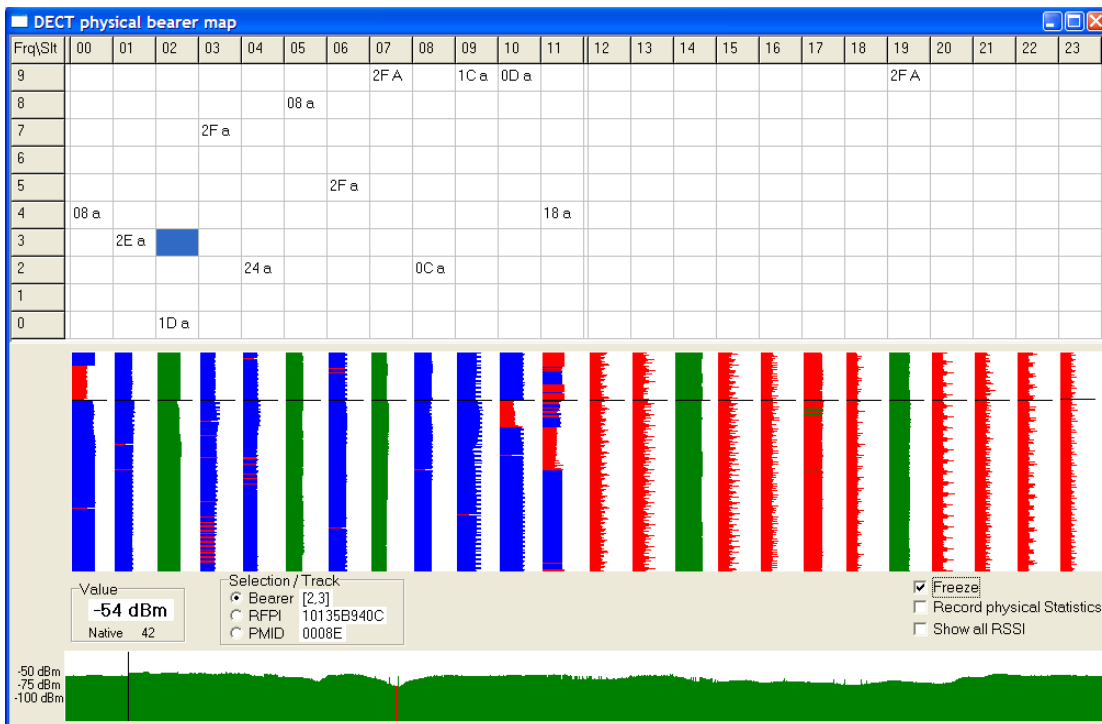
The lower status line shows:
- Current offset of Capture Unit within a complete DECT frame.
- Number of detected (Nt) dummy bearers and traffic bearer packets respectively.
- Number of detected packets which are not Nt.
- Number of unique RFPI detected.
- Currently detected RFPI.

2.2.2 DECT spectrum map

The DECT spectrum map is enabled by checking the *Scope* checkbox in the DECT system scanner pane. It shows asynchronous signal strength on the 10 DECT carriers versus time. The x-axis shows a 10 ms time period, which is not synchronous to any DECT system. When a FP is detected, is marked with a yellow vertical line and the detect RFPI is shown. The RFPI selected in the DECT scanner window is marked with red vertical line.

2.2.3 DECT physical bearer map

This pane shows physical slot/frequency positions of DECT bearers. It shows the 24 timeslots and the 10 carriers. If the analyzed system supports less than 10 carriers, these are left blank in the display. In the matrix is shown the RPN of any FP or PP in the network. DECT bearers that do not match the selected RFPI/PLI are not shown. Additionally the matrix cell may contain CRC information:

- **a:** A-field CRC is correct on dummy bearer (BA equals 111)
- **A:** A-field CRC is correct on traffic bearer (BA not equal 111)
- **x:** X-CRC correct on traffic bearer (in mode "Full Rx Info" only)

Below the bearer matrix is displayed physical measurements performed by the Capture Unit in each slot per frame. The physical parameter can be one of:

- Signal strength (RSSI)
- Bit timing
- Bit timing with 1/9 resolution (high resolution)

One horizontal line is display each frame. The display wraps around each 200 frames (2 seconds). The coloring of the lines corresponds to:

Red:	Incorrect A-CRC (no bearer)
Blue:	Dummy bearer or Q2=0
Green:	Traffic bearer and Q2=1
Yellow:	Traffic bearer and Q1=1

When selecting a cell in the matrix (left mouse click) the captured information from the selected bearer is extracted and shown in the graph below. The information field shows the selected RFPI and PMID as well as the capture physical parameter.
A reference bearer can be selected (or de-selected) by CTRL + left mouse button. The graph the shows the physical parameters difference between the selected bearer and the reference bearer.
Selectable options:

Option	Description
Selection / Track	o **Bearer**: Fixed slot/carrier position o **RFPI**: Automatic tracking of RFPI for bearer and reference bearer position o **PMID**: Automatic tracking of PMID for bearer and reference bearer position
Show RSSI	Forces display of RSSI level in the bearer matrix even for bearer positions where no bearers are detected.
Freeze	Freeze display content
Record physical Statistics	Record cell physical parameter for each RPN in a comma separated file.

Note: When "Full Rx Info" is selected only every 2nd slot contains information

2.2.4 DECT bearer information

This pane shows MAC bearer information. This display is only possible in PROTOCOL capture mode. In this mode, maximum one bearer can be collected per time slot. The following MAC information are displayed:

Column	Description
Slot	DECT timeslot
Freq	DECT RF carrier
RFPI	Radio Fixed Part Identity
RPN	Radio part Number
PMID	Portable MAC Identity
RSSI	Receiver Signal Strength Indication (dBm)
Dly	Delay (µs)
Head	A-field header value
BlindSlot	Blindslot information (MAC layer information)
DB	Dummy or C/L bearer position (see appendix for encoding)
Qh=0	Q-channel, Static system information
Qh=3	Q-channel, Fixed part capabilities
Qh=4	Q-channel, Extended fixed part capabilities

Qh=c	Q-channel, Extended fixed part capabilities (part 2)

2.2.5 DECT cell overview

```
■ DECT cell overview                                                                          □▣✕
          |  Rpn = x0   |  Rpn = x1   |  Rpn = x2   |  Rpn = x3   |  Rpn = x4   |  Rpn = x5   |  Rpn = x6   |  Rpn = x7
   Time   |0123456789ab |0123456789ab |0123456789ab |0123456789ab |0123456789ab |0123456789ab |0123456789ab |0123456789ab
----------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------
13:25:29.00 |           |             |             |             |      C      |             |             |
13:25:29.01 |           |             |             |             |      w      |             |             |
13:25:29.03 |     .     |        .  . |             |       .   . .|.     4 . . .|. .  .  .    |   .      . 9 . |  .
13:25:40.04 |           |             |             |             |C            |             |             |
13:25:40.05 |           |             |             |             |w            |             |             |
13:25:40.23 |       .   |      .   . .|       .     |      .    .  |.  . . .  . .|   .  .      |  .      . .9 1|

13:25:55.59 |           |    .     .  |             |  ...        |..  .    . . |  . . .      |  .      . 9 1|          .
```

Show bearer activity in different cells (RPN mod 8). The activity in the individual slots are shown in separate columns (12 columns per RPN)
Lower line a showing current status.

Legend	Description
C	MAC access_request
H	MAC handover request (bearer HO or connection HO)
w	MAC wait
a	MAC bearer_confirm
r	MAC release
0..9	Active traffic carrier
.	Dummy bearer

2.2.6 DECT protocol trace

This window is available in protocol mode only. Left side show FP transmission and right side shows PP transmission. Paging are shown in the middle. By default this window only shows messages that are relevant for connection oriented connections.

Display syntax:

```
TTTTTTTT.TT CS HHH  A-field                    CS HHH  A-field
------ -- --- ----------                       -- --- ----------
13:17:27.63                                     98 Mt--0068801102
13:17:27.91 98 Ct0-110101A734


Legend:
TTTTTTTT.TT Timestamp (from PC) with 10ms resolution
CS          Bearer postion; C=carrier, S=slot-pair
HHH         Messages type
A-field     A-field tail content (40 bits)


Lines without timestamp are interpretation of information above.
```

Display control can be configured using these options:

Selection	Description
Scroll	Display automatically scrolls when lines are shown
Pause	Stop protocol analyze, freeze display content
Time-PC	Display timestamp from PC
Time-Frame	Display Multiframenumber and Framenumber
Show all Pt	Force showing all Pt messages
Show Qt	Force showing Qt messages
Show Bfield	Show all the capture B-field (Note.: display may be overflowed on some PC)
Hide Nwk	Hide interpretation of NWK layer messages
Hide Dlc	Hide interpretation of DLC layer messages
Hide Ct	Hide MAC layer Ct messages
Hide Mt/Pt	Hide MAC layer Mt and Pt messages
Deep analysis	Interpretation and display of NWK information element fields
Scrambler	Un-scramble B-field payload
Act-B	Do only show Bfield in frames containing active signaling in the A-field.
F0on	Do only show Bfield info in frame 0, when used in combination with "Show Bfield"
CapaInfo	Dump current FP capability information
Set Mask	Set FMID and PMID filter mask in hexadecimal format.
Set FmidPmid	Set FMID and PMID filter in hexadecimal format.
Clear	Clear window content
CopyToClip	Copy window content to Windows clipboard.

When selecting Deep Analysis, the interpretation of NWK signaling is similar to example below:

B-field payload such as DECT-ULE packets may also be analyzed as shown example below:

3 Log files format

The DECT AirSpy can produce a number of log files. These logfiles can be opened and closed by checking or un-checking the check-field in the DECT AirSpy CTRL pane. When checking, empty files are opened and when un-checking the files are flushed and closed. More files may be open at the same time. The information logged in the files are independent of any display filtering.

3.1 Capture.log

Binary formatted file containing the native captured information from the Capture Unit.

3.2 DECT.log

This file is not produced directly by the AirSpy application, but is a result of converting the Capture.log binary file using the Convbin.exe tool.

```
TTT.TT Fn CS  Xs Sl   Ph   A-field       Xt Interpretation                  BA B-field
------ -- --  -- --   --   ------------  -- -------------------------        -- --------
103.43: 7(20) Bs 00:  38  6E10135B941C  Nt RFPI=10135B941C                    7:FFFFFFFF...
103.43: 7(61) Bs 01:  24  -- -- -- -- -- --
103.43: 7(22) Bs 02:  41  6E10135B940C  Nt RFPI=10135B940C                    7:FFFFFFFF...
103.43: 7(23) Bs 03:  38  6110135B941C  Nt RFPI=10135B941C                    7:FFFFFFFF...
103.43: 7(84) Bs 04:  20  -- -- -- -- -- --
```

```
103.43: 7(95) Bs 05:  32 6E10135B940F  Nt RFPI=10135B940F                        7:FFFFFFFF...
103.43: 7(26) Bs 06:  28  -- -- -- -- -- --
103.43: 7(58) Bs 08:  44 6E10135B942E  Nt RFPI=10135B942E                        7:FFFFFFFF...
103.43: 7(19) Bs 09:  37 6E10135B9418  Nt RFPI=10135B9418                        7:FFFFFFFF...
103.43: 7(7a) Bs 10:  38 6E10135B9409  Nt RFPI=10135B9409                        7:FFFFFFFF...
103.43: 7(5b) Bs 11:  26  -- -- -- -- -- --
103.43: 7(23) Hs 15:  41 6110135B941C  Nt RFPI=10135B941C
103.44: 8(20) Bs 00:  38 8E0003FF0201  Qt SN=0   CN=2   Prim.Scan.=1
103.44: 8(61) Bs 01:  23  -- -- -- -- -- --
103.44: 8(22) Bs 02:  42 8E0203FF0201  Qt SN=2   CN=2   Prim.Scan.=1
103.44: 8(23) Bs 03:  46 810303FF0201  Qt SN=3   CN=2   Prim.Scan.=1
103.44: 8(84) Bs 04:  20  -- -- -- -- -- --
103.44: 8(95) Bs 05:  32 8E0503FF0901  Qt SN=5   CN=9   Prim.Scan.=1
103.44: 8(26) Bs 06:  29  -- -- -- -- -- --
103.44: 8(58) Bs 08:  44 8E6F0FCBA166  Qt Multiframe number=CBA166
103.44: 8(19) Bs 09:  37 8E4010000010  Qt Extended Fixed Capability=01000
103.44: 8(7a) Bs 10:  39 8E4010000010  Qt Extended Fixed Capability=01000
103.44: 8(5b) Bs 11:  26  -- -- -- -- -- --
103.44: 8(23) Hs 15:  40 6110135B941C  Nt RFPI=10135B941C
103.44: 8(0a) Hs 22:  49 E1004180008E   first Mt basic access_request FMID=418 PMID=0008E
103.45: 9(20) Bs 00:  46 6E10135B941C  Nt RFPI=10135B941C
103.45: 9(61) Bs 01:  23  -- -- -- -- -- --
103.45: 9(22) Bs 02:  45 6E10135B940C  Nt RFPI=10135B940C
103.45: 9(23) Bs 03:  38 6110135B941C  Nt RFPI=10135B941C
103.45: 9(84) Bs 04:  21  -- -- -- -- -- --
103.45: 9(95) Bs 05:  32 6E10135B940F  Nt RFPI=10135B940F
103.45: 9(26) Bs 06:  28  -- -- -- -- -- --
103.45: 9(58) Bs 08:  45 6E10135B942E  Nt RFPI=10135B942E
103.45: 9(19) Bs 09:  38 6E10135B9418  Nt RFPI=10135B9418
103.45: 9(0a) Bs 10:  38 C1054180008E  Mt basic wait FMID=418 PMID=0008E
103.45: 9(5b) Bs 11:  26  -- -- -- -- -- --
103.45: 9(23) Hs 15:  46 6110135B941C  Nt RFPI=10135B941C
103.45: 9(0a) Hs 22:  49 6110135B9418  Nt RFPI=10135B9418
103.46:10(20) Bs 00:  46 EE0B941C3302  Pt FMID=xxxxxB941C Recomm other bea SN=3 CN=2
103.46:10(61) Bs 01:  21  -- -- -- -- -- --
103.46:10(22) Bs 02:  44 6E10135B940C  Nt RFPI=10135B940C
103.46:10(23) Bs 03:  38 6110135B941C  Nt RFPI=10135B941C
103.46:10(84) Bs 04:  21  -- -- -- -- -- --
103.46:10(95) Bs 05:  32 6E10135B940F  Nt RFPI=10135B940F
103.46:10(26) Bs 06:  27  -- -- -- -- -- --
103.46:10(58) Bs 08:  44 6E10135B942E  Nt RFPI=10135B942E
103.46:10(19) Bs 09:  39 6E10135B9418  Nt RFPI=10135B9418
103.46:10(0a) Bs 10:  37 6110135B9418  Nt RFPI=10135B9418
103.46:10(5b) Bs 11:  26 6E10135B940A  Nt RFPI=10135B940A
103.46:10(23) Hs 15:  41 6110135B941C  Nt RFPI=10135B941C
103.46:10(0a) Hs 22:  49 C1054180008E  Mt basic wait FMID=418 PMID=0008E
103.47:11(20) Bs 00:  37 6110135B941C  Nt RFPI=10135B941C
103.47:11(61) Bs 01:  22  -- -- -- -- -- --
103.47:11(22) Bs 02:  41 6E10135B940C  Nt RFPI=10135B940C
103.47:11(23) Bs 03:  38 6110135B941C  Nt RFPI=10135B941C
103.47:11(84) Bs 04:  21  -- -- -- -- -- --
103.47:11(95) Bs 05:  33  -- -- -- -- -- --
103.47:11(26) Bs 06:  29  -- -- -- -- -- --
103.47:11(58) Bs 08:  44 6E10135B942E  Nt RFPI=10135B942E
103.47:11(19) Bs 09:  38 6E10135B9418  Nt RFPI=10135B9418
103.47:11(0a) Bs 10:  38 C1044180008E  Mt basic bearer_confirm FMID=418 PMID=0008E
103.47:11(5b) Bs 11:  25  -- -- -- -- -- --
103.47:11(32) Hs 14:  29 6110135B941B  Nt RFPI=10135B941B
103.47:11(23) Hs 15:  46 6110135B941C  Nt RFPI=10135B941C
103.47:11(0a) Hs 22:  49 6110135B9418  Nt RFPI=10135B9418
103.48:12(20) Bs 00:  38 EE0B941C3302  Pt FMID=xxxxxB941C Recomm other bea SN=3 CN=2
103.48:12(61) Bs 01:  21  -- -- -- -- -- --
103.48:12(22) Bs 02:  41 6E10135B940C  Nt RFPI=10135B940C
103.48:12(23) Bs 03:  38 6110135B941C  Nt RFPI=10135B941C
103.48:12(84) Bs 04:  20  -- -- -- -- -- --
103.48:12(95) Bs 05:  33  -- -- -- -- -- --
103.48:12(26) Bs 06:  28  -- -- -- -- -- --
103.48:12(58) Bs 08:  44 6E10135B942E  Nt RFPI=10135B942E
103.48:12(19) Bs 09:  38 6E10135B9418  Nt RFPI=10135B9418
103.48:12(0a) Bs 10:  38 6110135B9418  Nt RFPI=10135B9418
103.48:12(5b) Bs 11:  25 6E10135B940A  Nt RFPI=10135B940A
103.48:12(42) Hs 14:  29  -- -- -- -- -- --
103.48:12(23) Hs 15:  46 6110135B941C  Nt RFPI=10135B941C
103.48:12(0a) Hs 22:  49 C137180F0F0F  Mt quality control FMID=180 PMID=F0F0F
```

```
103.49:13(20) Bs 00:  46 6E10135B941C  Nt RFPI=10135B941C
103.49:13(61) Bs 01:  21  -- -- -- -- -- --
103.49:13(22) Bs 02:  45 6E10135B940C  Nt RFPI=10135B940C
103.49:13(23) Bs 03:  38 6110135B941C  Nt RFPI=10135B941C
103.49:13(95) Bs 05:  33 6E10135B940F  Nt RFPI=10135B940F
103.49:13(58) Bs 08:  45 6E10135B942E  Nt RFPI=10135B942E
103.49:13(19) Bs 09:  38 6E10135B9418  Nt RFPI=10135B9418
103.49:13(0a) Bs 10:  37 6110135B9418  Nt RFPI=10135B9418
103.49:13(5b) Bs 11:  26 6E10135B940A  Nt RFPI=10135B940A
103.49:13(52) Hs 14:  35  -- -- -- -- -- --
103.49:13(23) Hs 15:  46 6110135B941C  Nt RFPI=10135B941C
103.49:13(0a) Hs 22:  49 6110135B9418  Nt RFPI=10135B9418
103.50:14(20) Bs 00:  46 6E10135B941C  Nt RFPI=10135B941C
103.50:14(61) Bs 01:  21  -- -- -- -- -- --
103.50:14(22) Bs 02:  45 6E10135B940C  Nt RFPI=10135B940C
103.50:14(23) Bs 03:  38 6110135B941C  Nt RFPI=10135B941C
103.50:14(95) Bs 05:  33 6E10135B940F  Nt RFPI=10135B940F
103.50:14(58) Bs 08:  45 6E10135B942E  Nt RFPI=10135B942E
103.50:14(19) Bs 09:  38 6E10135B9418  Nt RFPI=10135B9418
103.50:14(0a) Bs 10:  38 6110135B9418  Nt RFPI=10135B9418
103.50:14(5b) Bs 11:  26 6E10135B940A  Nt RFPI=10135B940A
103.50:14(62) Hs 14:  32  -- -- -- -- -- --
103.50:14(23) Hs 15:  41 6110135B941C  Nt RFPI=10135B941C
103.50:14(0a) Hs 22:  49 C137180F0F0F  Mt quality control FMID=180 PMID=F0F0F
103.51:15(20) Bs 00:  37 6E10135B941C  Nt RFPI=10135B941C
103.51:15(61) Bs 01:  21  -- -- -- -- -- --
103.51:15(22) Bs 02:  41 6E10135B940C  Nt RFPI=10135B940C
103.51:15(23) Bs 03:  38 6110135B941C  Nt RFPI=10135B941C
103.51:15(95) Bs 05:  32  -- -- -- -- -- --
103.51:15(58) Bs 08:  44 6E10135B942E  Nt RFPI=10135B942E
103.51:15(19) Bs 09:  37 6E10135B9418  Nt RFPI=10135B9418
103.51:15(0a) Bs 10:  38 6110135B9418  Nt RFPI=10135B9418
103.51:15(5b) Bs 11:  25 6E10135B940A  Nt RFPI=10135B940A
103.51:15(23) Hs 15:  41 6110135B941C  Nt RFPI=10135B941C
103.51:15(0a) Hs 22:  49 6110135B9418  Nt RFPI=10135B9418
103.52: 0(20) Bs 00:  46 EE0B941C3302  Pt FMID=xxxxxB941C Recomm other bea SN=3 CN=2
103.52: 0(61) Bs 01:  21  -- -- -- -- -- --
103.52: 0(22) Bs 02:  45 EE0B940CB210  Pt FMID=xxxxxB940C Active carriers:210
103.52: 0(23) Bs 03:  37 E10B941C4207  Pt FMID=xxxxxB941C Good RFP bea SN=2 CN=7
103.52: 0(95) Bs 05:  33  -- -- -- -- -- --
103.52: 0(58) Bs 08:  44 EE0B942EA00F  Pt FMID=xxxxxB942E RFP status: Clear
103.52: 0(19) Bs 09:  38 6E10135B9418  Nt RFPI=10135B9418
103.52: 0(0a) Bs 10:  38 6110135B9418  Nt RFPI=10135B9418
103.52: 0(5b) Bs 11:  26 EE0B940A93FF  Pt FMID=xxxxxB940A Bearer HO info
103.52: 0(23) Hs 15:  41 6110135B941C  Nt RFPI=10135B941C
103.52: 0(0a) Hs 22:  49 C137180F0F0F  Mt quality control FMID=180 PMID=F0F0F
```

If B-field payload is captured, it is also available in the DECT.log file (very long lines!). :

Legend:

TTT.TT	**Timestamp in seconds with 10ms resolution**
Fn	**Framenumber, 0..15**
CS	**Bearer, carrier and slot-pair, see appendix**
Xs	**Sending part Bs or Hs**
Sl	**Slotnumber, 0..23**
Ph	**Physical parameter, RSSI or timing**

```
A-field        A-field content, head and tail, totally 48 bits
Xt             Message type defined by header
BA             BA field from the A-field header
B-field        RAW B-field payload. If the R-CRC check passes for the
               individual subfields or the complete B-field, they are
               separated by a ".".
```

3.3 FORMAT.log

Tbd.

3.4 MAC.log

Extracted MAC layer information:

```
TTT.TT     CS HHH  A-field                    CS HHH  A-field
------     -- ---  ----------                 -- ---  ----------
417.92     22 Pt   DEC07E0630
417.94     22 Pt   C001A47EEE
417.96     22 Pt   61480EFFFF
420.07                                        96 Mt   0068801102
420.08     96 Mt   0568801102
420.08                                        96 Mt   0568801102
420.09     96 Mt   0468801102
420.16                                        96 Ct1  910001A6B7
420.21     96 Ct1  91210145F5
420.30                                        96 Ct0  1102590305
420.32                                        96 Ct1  050780A800
420.34                                        96 Ct0  07E0092E06
420.36                                        96 Ct1  07A0A50007
420.38                                        96 Ct0  E01688E090
420.40                                        96 Ct1  F0F0F0111B
420.45     96 Ct0  110101A734
420.55     96 Ct1  130019830D
420.59     96 Ct0  1E028089F0
420.63     96 Ct1  F0F0F084BD
420.70                                        96 Ct0  1321015F7E
420.75     96 Ct0  130211837B
420.77     96 Ct1  E400F0C92E
420.90                                        96 Ct1  112015037B
420.92                                        96 Ct0  2C01332D9C
420.96                                        96 Ct1  130101BF3E
420.97     96 Ct0  1121014774
421.07     96 Ct1  132011837B
421.11     96 Ct0  E43FF03B7F
421.18                                        96 Ct0  1321015F7E
421.28     96 Pt   1C11031A8A
422.08     96 Pt   1C11031A8A
422.28                                        96 Ct1  112211034D
422.30                                        96 Ct0  E200F0CAB9
422.37     96 Ct1  110101A734
422.49     96 Ct0  130211835A
422.51     96 Ct1  E210F047C3
422.58                                        96 Ct1  130101BF3E
422.63     96 Mt   0F68801102
422.64     96 Mt   0F68801102
```

```
Legend:
TTT.TT         Timestamp in seconds with 10ms resolution
CS             Bearer, carrier and slot-pair, see appendix
HHH            Messages type defined by header
A-field        A-field tail content (40 bits)
```

3.5 CellStat.log

Cell physical statistics can only recorded in CELL scanning mode. It is a comma separated file intended for import into MS Excel for analyse and presentation.

```
83.80 ,35,,,,,,,,,,,,,,,,,,,,,34,,27,,45,39,,,,,29,,,,,,,,32,,,43,36
83.90 ,,,,,,,,,38,,33,46,30,30,,,,,,,,,,37,,25,35,47,35,30,,,,,,,,,,,,32,32,,,43,29
84.00 ,,,,,,,,,33,38,25,25,40,31,28,33,,,,,,,,,34,33,28,34,44,38,26,,,,,29,,,,,,,35,32,,,42,36
84.10 ,,,,,,,,,34,36,26,28,38,32,,34,,,,,,,,,34,27,28,34,44,38,26,,,,,29,,,,,,,34,32,,,42,35
84.20 ,35,,,,,,,,,37,27,33,45,30,29,28,,,,,,,,,34,,26,35,44,38,,,,,,29,,,,,,,32,32,,,42,35
84.30 ,,,,,,,,,38,27,34,46,30,29,28,,,,27,,,,,37,,26,35,47,35,30,,,,,,,,,,32,32,,,43,29
84.40 ,,,,,,,,,32,39,26,34,45,29,30,,,,,,,,,,37,,28,35,46,35,31,,,,,,,,,,,31,32,,,43,29
84.50 ,,,,,,,,,33,35,,31,38,31,,34,,,,,,,,,,34,,28,35,44,38,,,,,,29,,,,,,34,32,,,43,35
84.60 ,,,,,,,,,,39,27,34,45,29,29,,,,,,,,,,38,,,35,46,35,30,,,,,,,,,,,32,33,,,43,28
84.70 ,,,,,,,,,34,39,26,26,45,29,26,29,,,,27,,,,,38,,27,35,47,35,29,,,,,,,,,,,32,32,,,43,29
84.80 ,,,,,,,,,33,36,26,,39,31,27,33,,,,,,,,,35,33,27,35,45,38,25,,,,,28,,,,,,,34,33,,,43,35
84.90 ,26,,,,,,,,34,35,25,28,39,31,27,32,,,,,,,,,34,33,28,35,46,38,26,,,,,28,,,,,,,35,33,,,42,35
85.00 ,35,,,,,,,,,36,26,34,45,28,29,,,,,,,,,,34,,,36,46,38,26,,,,,29,,,,,,,30,33,,,42,35
85.10 ,,,,,,,,,32,39,27,34,45,29,29,,,,,,,,,,38,,,36,44,35,30,,,,,24,,,,,,,30,32,,,43,29
85.20 ,,,,,,,,,34,36,26,28,39,32,,33,,,,,,,,,34,,,35,46,39,26,,,,,29,30,,,,,,34,33,,,42,35
85.30 ,26,,,,,,,,32,36,,34,46,30,29,,,,,,,,,,35,,,37,44,36,29,,,,,28,,,,,,,30,32,,,43,35
85.40 ,36,,,,,,,,,31,39,,34,46,30,29,,,,,,26,,,,,38,,,37,44,36,29,,,,,,,,,,,30,32,,,43,29
85.50 ,,,,,,,,,34,39,,,31,45,29,,30,,,,,27,,,,,38,,,36,44,36,30,,,,,,,,,,,,32,32,,,43,29
85.60 ,,,,,,,,,34,35,26,32,38,32,,34,,,,,,,,,36,33,,36,46,39,26,,,,,28,,,,,,,35,33,,,42,36
85.70 ,24,,,,,,,,36,26,32,38,32,29,34,,,,,,,,,,36,32,,36,46,38,26,,,,,28,,,,,,,36,33,,,42,36
85.80 ,35,,,,,,,,32,39,,34,45,30,30,30,,,,27,,,,,39,,,37,44,35,29,,,,,24,30,,,,,,32,31,,,43,29
```

4 Installation guide

Install USB driver
Install the DECT AirSpy application
Connect Capture Unit before starting PC application software

5 Limitations and known problems

The Capture Unit has one RF section only (no capture on multiple carriers per slot)
Slow RF synthesis allow 2 operation configuration:

- o   Blind slot (full slot)
- o   Zero blind slot (A-field only)

The RF section is un-calibrated; hence RSSI values are not accurate
Only A-field signalling and fullslot B-field when using "Full Rx Info" are captured.
Encrypted DLC and NWK messages can not be decoded
The Capture Unit may be overflowed if there lot of signalling on all timeslot for many frames, especially when B-field capture is also enabled. It is advisable only to enable B-field capture and specific BA values of interest.
The Capture Unit operates in slots only. It is not possible to analyse RF outside slot/frame format.
Due to communication bandwidth (230kbaud) on the serial link from the Capture Unit, either RSSI or timing information is captured in "All slots" mode.
Reset of Capture Unit by unplugging and plugging may be necessary in some cases when capturing many cells in protocol mode.

6 Glossary

Ct   Control channel tail message (for DLC and NWK layers)
DLC   Data Link Control
FMID   Fixed MAC Identity
MAC   Medium Access Control
Mt   MAC layer tail message
Nt   Network identity tail message (RFPI)
NWK   Network
PLI   PARK Length Indicator
PMID   Portable MAC Identity
PSCN   Primary receive Scan Carrier Number
Pt   Paging message tail
Qt   System information tail (Q-channel)
RF   Radio Frequency
RFPI   Radio Fixed Part Identity
RPN   Radio Part Number
RSSI   Receiver Signal Strength Indication

7 Appendixes.

7.1 Bearer encoding:

CS:
C=carrier;   range: 0,1,2,3,4,5,6,7,8,9
S=slot-pair; range: 0,1,2,3,4,5,6,7,8,9,A,B