P25 ADP/ARC4 KEY FINDER
for
RASPBERRY PI 1/2/3/4

<u>Disclaimer</u>: This software must be used on your own radios in your test lab. Do not use this software on radios that do not belong to you, it is illegal in most countries. Check your local legislation.

This software allows you to find the key for Motorola P25 ADP / ARC4-40.

I am not the author of this software, I explain to you what I understood about how it works.

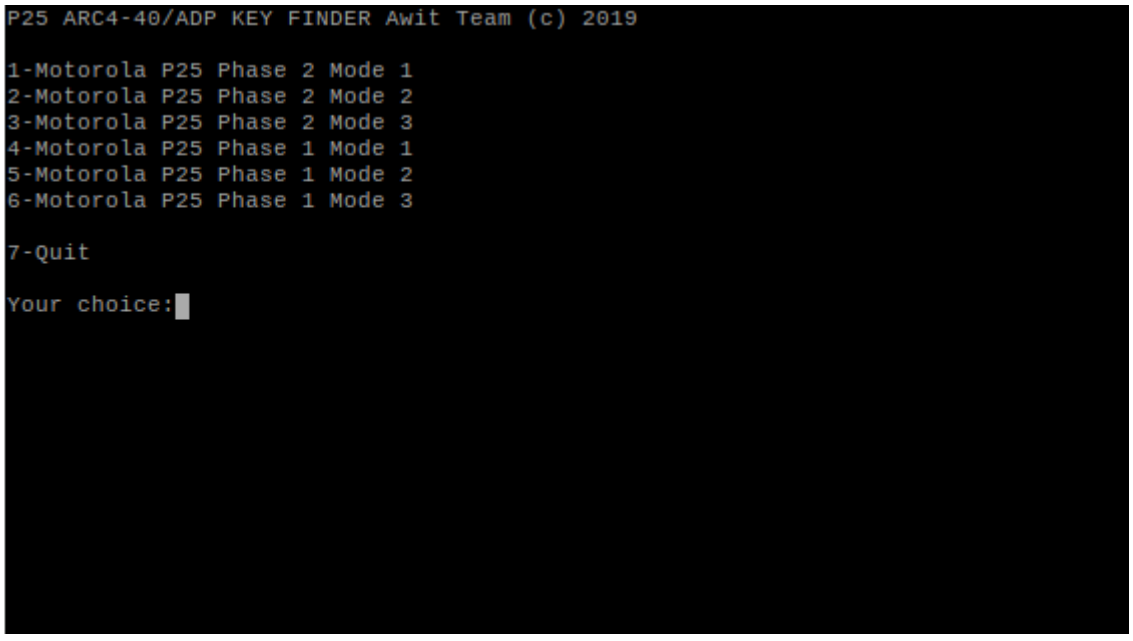
There are two pieces of software: a 32-bit version and a 64-bit version, depending on the operating system you have on your Rasbperry Pi.
The 64-bit version is faster than the 32-bit version.

Verify that the program has execution rights. If it does not have them, set the execution rights, such as:

sudo chmod 777 p25keyfinder

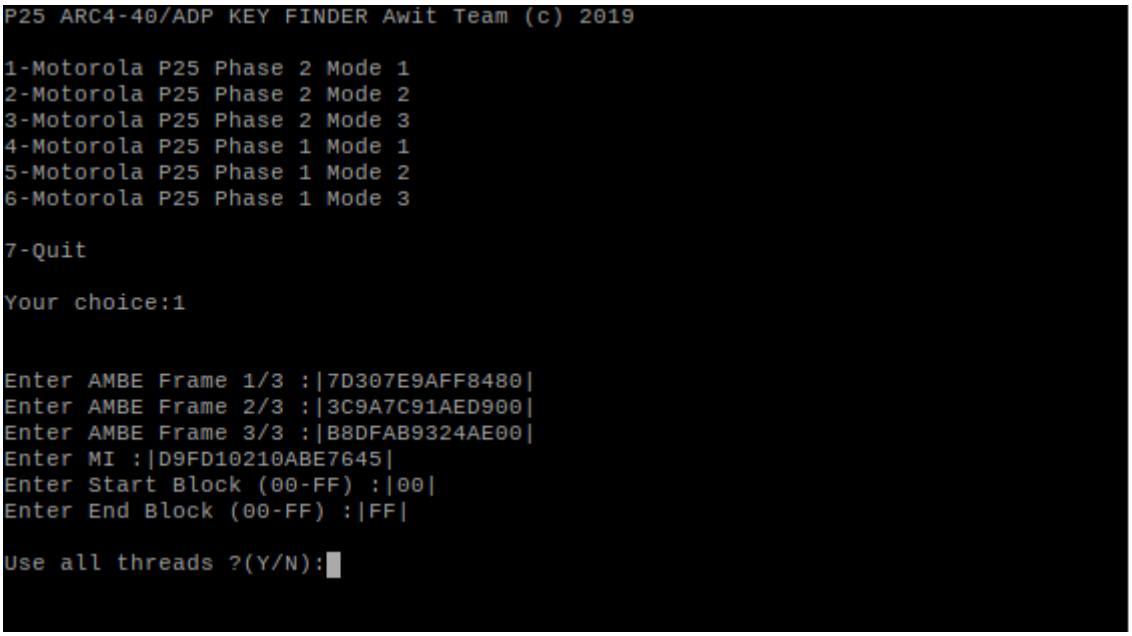
If the program finds a key, it writes it to the **keys_found.txt** file (the file does not exist and will be created when a key is found). Check that write permissions are possible by the program or run the program in root mode:

sudo ./p25keyfinder



<u>Option 1 (P25 Phase 2):</u>

Enter the 3 frames:
<u>The MI, Start Block : 00 and End Block : FF</u>

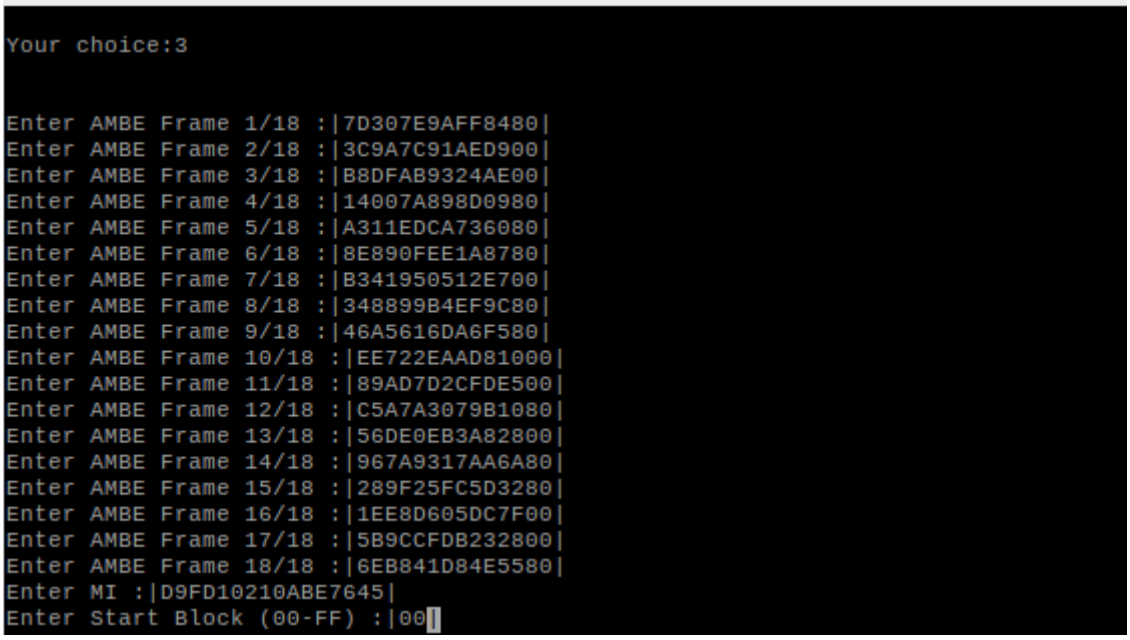


You can use all the threads available on your Raspberry Pi: answer **Yes**

Or all threads minus one: answer **No** (if you want to continue using the Raspberry Pi to do something else).

Option 3 (P25 Phase 2):

Enter the 18 frames:



You can stop the search and resume it later. For example, you searched for blocks from 00 to 4F (hexadecimal) and stopped the search and turned off the Raspberry Pi.

Another day you can resume the search from 4F. You put 4F in the start block (you have to put the frames back because the program doesn't keep them in memory):

If the program finds a key, it writes it to the **keys_found.txt** file (the file does not exist and will be created when a key is found). Check that write permissions are possible by the program or run the program in root mode:

sudo ./p25keynfinder

Option 4 (P25 Phase 1):

Enter the frame:
The MI, Start Block : 00 and End Block : FF

```
P25 ARC4-40/ADP KEY FINDER Awit Team (c) 2019

1-Motorola P25 Phase 2 Mode 1
2-Motorola P25 Phase 2 Mode 2
3-Motorola P25 Phase 2 Mode 3
4-Motorola P25 Phase 1 Mode 1
5-Motorola P25 Phase 1 Mode 2
6-Motorola P25 Phase 1 Mode 3

7-Quit

Your choice:4


Enter IMBE Frame 1/1 :|6D54EB24A86E4A68B51498|
Enter MI :|0B62456F3D3E4B03|
Enter Start Block (00-FF) :|00|
Enter End Block (00-FF) :|FF|

Use all threads ?(Y/N):
```

Option 6 (P25 Phase 1):

Enter the 18 frames:
The MI, Start Block : 00 and End Block : FF

```
Your choice:6


Enter IMBE Frame 1/18 :|6D54EB24A86E4A68B51498|
Enter IMBE Frame 2/18 :|9A770A7B2D7E75F9879AEC|
Enter IMBE Frame 3/18 :|C6506EBCC4809CCFAB8069|
Enter IMBE Frame 4/18 :|4E69800822362F0501E947|
Enter IMBE Frame 5/18 :|C396D54BF10845ECC7FD9F|
Enter IMBE Frame 6/18 :|4D8AA1FF0A4056708C43C1|
Enter IMBE Frame 7/18 :|66F6413DA5A97D44F5640A|
Enter IMBE Frame 8/18 :|BF6BF0F048BC174ED72071|
Enter IMBE Frame 9/18 :|0ACF7A812C02BA32122FCD|
Enter IMBE Frame 10/18 :|D430F6186FF00127A38529|
Enter IMBE Frame 11/18 :|704FEFEF2838444DA875DD|
Enter IMBE Frame 12/18 :|2CDF2885EEB0FAA38BBF18|
Enter IMBE Frame 13/18 :|4F3503E97D7B2FE178EA0F|
Enter IMBE Frame 14/18 :|BA07269DB8A5265D04CC57|
Enter IMBE Frame 15/18 :|BCF7414B6F0C7F24B31B63|
Enter IMBE Frame 16/18 :|1BDEAAF7CF2BFA1EB3FA0F|
Enter IMBE Frame 17/18 :|8340356BF95C9C768167F6|
Enter IMBE Frame 18/18 :|7672726E489547D115986D|
Enter MI :|0B62456F3D3E4B03|
Enter Start Block (00-FF) :|00|
```

How do I get P25 ARC4 frames?

Use DSD-FME.

To get help:

dsd-fme.exe -h

dsd-fme -Z

If you have too many receive errors, DSD-FME allows you to capture directly from an RTL-SDR dongle:

Frequency capture 432.153 Mhz :

dsd-fme.exe -Z -i rtl:1:432.153M:22:-2:12:0:6021

You may need to fine-tune the frequency : 432.151, 432.152, 432.154, 432.155 ...

You can use 2>log.txt to save the screen output to a text file.

dsd-fme.exe -Z -i rtl:1:432.153M:22:-2:12:0:6021 2>log.txt

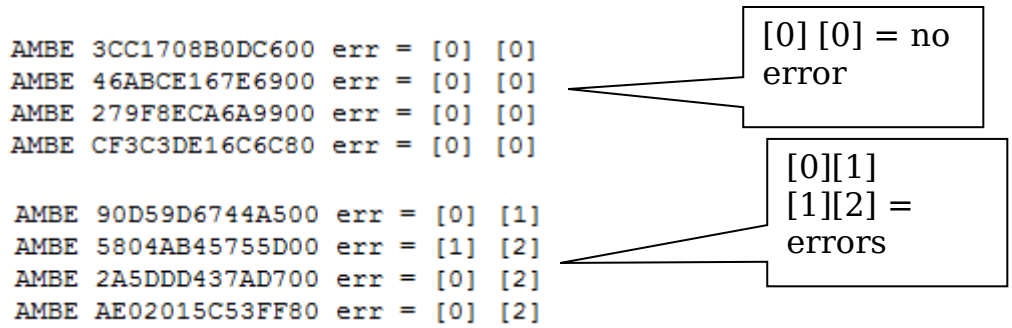
You must use the first 1, 3 or 18 frames of an ARC4 transmission, but be careful, you have to start at first superframe of the transmission.

For P25 Phase 2 you must add : -X

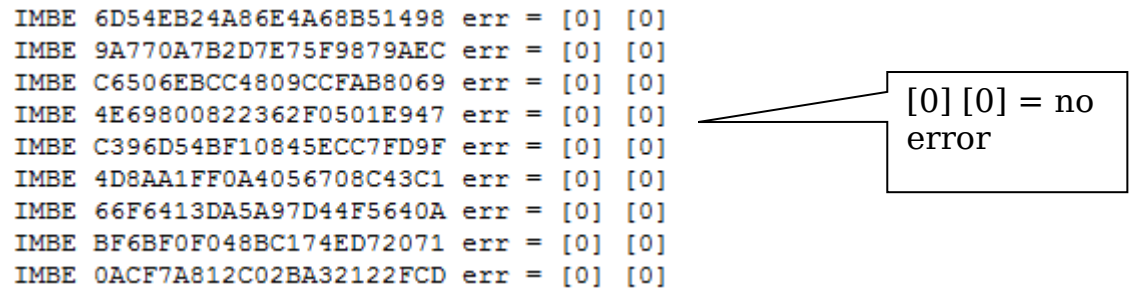
dsd-fme.exe -Z -X -X BEE00ABC123 -i rtl:1:432.153M:22:-2:12:0:6021 2>log.txt

-X <hex> Manually Set P2 Parameters (WACN, SYSID, CC/NAC) (-X BEE00ABC123)

It is necessary to ensure that the errors are at 0: (P25 Phase 2)



It is necessary to ensure that the errors are at 0: (P25 Phase 1)



If you have errors : start again, don't waste your time with frames with errors. The ARC4 is very sensitive, a simple error in receiving can prevent the key from being found.

You need to look for the first 1 or 3 frames of the superframe of a transmission (options 1, 2, 4, 5) or the first 18 frames (for options 3 and 6),

For P25 Phase 1 you should always look for "**HDU**" in the DSD-FME log files.
For P25 Phase 2 you should always look for "**MAC_PTT**" in the DSD-FME log files.

HDU

AA for ALG_ID = ADP / ARC4

MI=0B62456F3D3E4B03

P25 Phase 1:

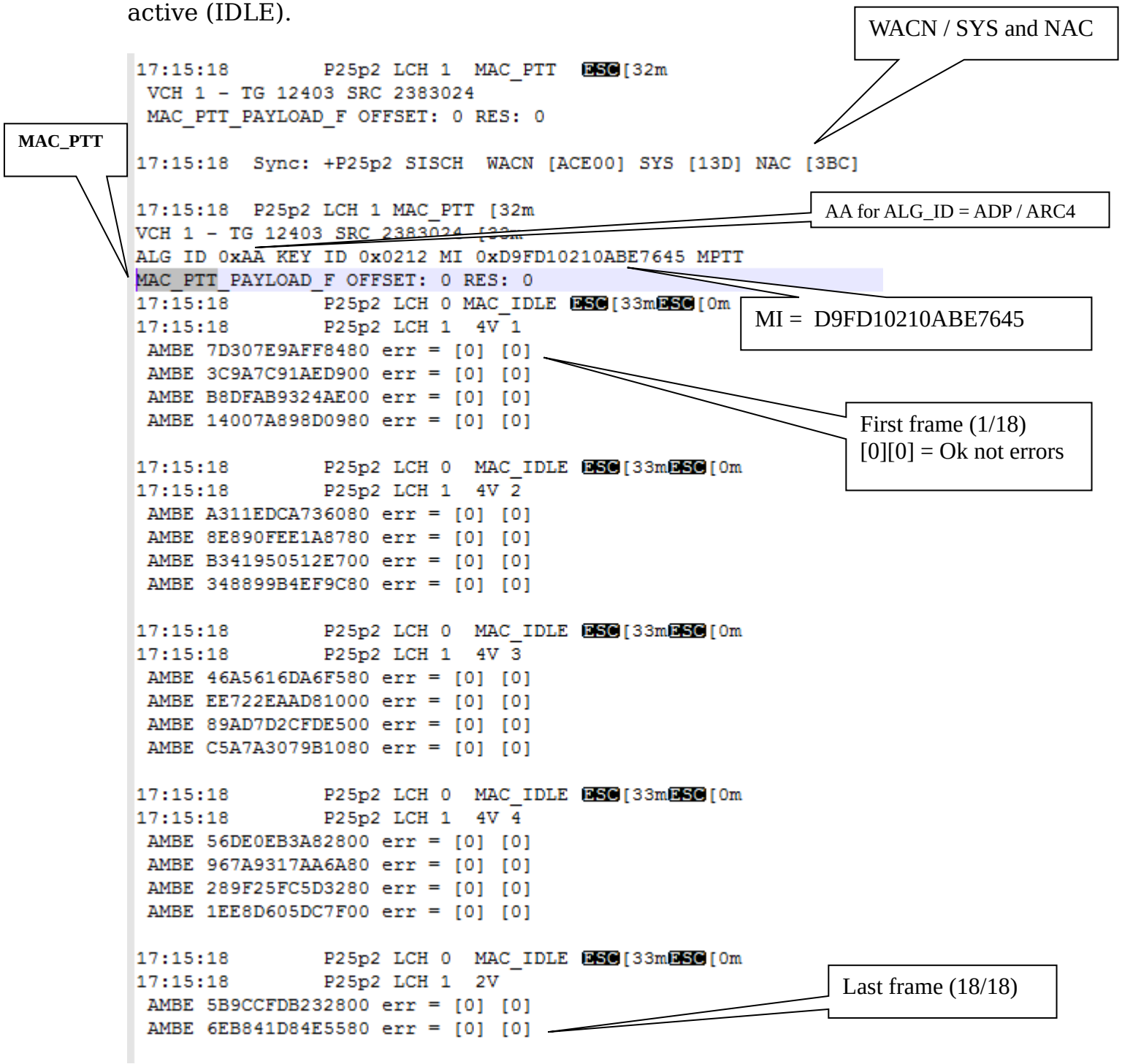
```
 LCW Conventional Fallb   Indication
13:10:34 Sync: -P25p1  nac: [ 1F7] src: [       0] tg: [ 2302]  TDU
13:10:34 Sync: -P25p1  nac: [ 1F7] src: [       0] tg: [    0]  HDU
 HDU  ALG_ID: 0xAA KEY_ID: 0x0001 MI: 0x0B62456F3D3E4B03 ENC
10:40:42 Sync: -P25p1  nac: [ 1F7] src: [       0] tg: [    0]  LDU1
 IMBE 6D54EB24A86E4A68B51498 err = [0] [0]
 IMBE 9A770A7B2D7E75F9879AEC err = [0] [0]
 IMBE C6506EBCC4809CCFAB8069 err = [0] [0]
 IMBE 4E69800822362F0501E947 err = [0] [0]
 IMBE C396D54BF10845ECC7FD9F err = [0] [0]
 IMBE 4D8AA1FF0A4056708C43C1 err = [0] [0]
 IMBE 66F6413DA5A97D44F5640A err = [0] [0]
 IMBE BF6BF0F048BC174ED72071 err = [0] [0]
 IMBE 0ACF7A812C02BA32122FCD err = [0] [0]
 LCW Encrypted Circuit Priority 4 Group Voice Channel User - Group 2302 Source 0
10:40:42 Sync: -P25p1  nac: [ 1F7] src: [       0] tg: [ 2302]  LDU2
 IMBE D430F6186FF00127A38529 err = [0] [0]
 IMBE 704FEFEF2838444DA875DD err = [0] [0]
 IMBE 2CDF2885EEB0FAA38BBF18 err = [0] [0]
 IMBE 4F3503E97D7B2FE178EA0F err = [0] [0]
 IMBE BA07269DB8A5265D04CC57 err = [0] [0]
 IMBE BCF7414B6F0C7F24B31B63 err = [0] [0]
 IMBE 1BDEAAF7CF2BFA1EB3FA0F err = [0] [0]
 IMBE 8340356BF95C9C768167F6 err = [0] [0]
 IMBE 7672726E489547D115986D err = [0] [0]
```

First frame (1/18)
[0][0] = Ok not errors

Last frame (18/18)

P25 Phase 2:

Phase 2 can carry two simultaneous voices : LCH 0 and LCH 1. If the two are active you should not mix them, only take care of LCH 0 or only LCH 1. In the example below, mixing is not possible because LCH 0 is not active (IDLE).




```
17:15:18        P25p2 LCH 1  MAC_PTT  ESC[32m
 VCH 1 - TG 12403 SRC 2383024
 MAC_PTT_PAYLOAD_F OFFSET: 0 RES: 0

17:15:18  Sync: +P25p2 SISCH  WACN [ACE00] SYS [13D] NAC [3BC]

17:15:18  P25p2 LCH 1 MAC_PTT [32m
VCH 1 - TG 12403 SRC 2383024 [32m
ALG ID 0xAA KEY ID 0x0212 MI 0xD9FD10210ABE7645 MPTT
MAC_PTT_PAYLOAD_F OFFSET: 0 RES: 0
17:15:18        P25p2 LCH 0 MAC_IDLE ESC[33mESC[0m
17:15:18        P25p2 LCH 1  4V 1
 AMBE 7D307E9AFF8480 err = [0] [0]
 AMBE 3C9A7C91AED900 err = [0] [0]
 AMBE B8DFAB9324AE00 err = [0] [0]
 AMBE 14007A898D0980 err = [0] [0]

17:15:18        P25p2 LCH 0  MAC_IDLE ESC[33mESC[0m
17:15:18        P25p2 LCH 1  4V 2
 AMBE A311EDCA736080 err = [0] [0]
 AMBE 8E890FEE1A8780 err = [0] [0]
 AMBE B341950512E700 err = [0] [0]
 AMBE 348899B4EF9C80 err = [0] [0]

17:15:18        P25p2 LCH 0  MAC_IDLE ESC[33mESC[0m
17:15:18        P25p2 LCH 1  4V 3
 AMBE 46A5616DA6F580 err = [0] [0]
 AMBE EE722EAAD81000 err = [0] [0]
 AMBE 89AD7D2CFDE500 err = [0] [0]
 AMBE C5A7A3079B1080 err = [0] [0]

17:15:18        P25p2 LCH 0  MAC_IDLE ESC[33mESC[0m
17:15:18        P25p2 LCH 1  4V 4
 AMBE 56DE0EB3A82800 err = [0] [0]
 AMBE 967A9317AA6A80 err = [0] [0]
 AMBE 289F25FC5D3280 err = [0] [0]
 AMBE 1EE8D605DC7F00 err = [0] [0]

17:15:18        P25p2 LCH 0  MAC_IDLE ESC[33mESC[0m
17:15:18        P25p2 LCH 1  2V
 AMBE 5B9CCFDB232800 err = [0] [0]
 AMBE 6EB841D84E5580 err = [0] [0]
```

A particularity of the P25 in relay mode exists: if the walkie-talkie is far from the relay, its transmission can arrive with errors.

The relay will send this data back with errors but as it is a new emission it sends the data received with error into data without error (but without really correcting them).

If you listen to the output relay you may believe that there are no errors (display err = [0] [0]) when there are errors inside the data because the frames received by the relay were bad.

The key will then never be found with these frames.

To be sure that there are no errors, you have to listen to the input relay (before the relay rebroadcasts). If you capture frames with err = [0] [0] in the input relay then you can be sure that there are no errors.

Troubleshooting P25 Phase 2:

The signal I receive is very good but I have errors like this all the time, why?

```
17:21:07 Sync: +P25p2 SISCH  WACN [BEE00] SYS [49A] NAC [49A]
17:21:07         P25p2 SACCH  R-S ERR Ss
17:21:07         P25p2 SACCH  R-S ERR Ss
17:21:07         P25p2 LCH 0  R-S ERR Fs
17:21:07         P25p2 LCH 1  DUID ERR -1
17:21:07 Sync: +P25p2 SISCH  WACN [BEE00] SYS [49A] NAC [49A]
17:21:07         P25p2 LCH 0  R-S ERR Fs
17:21:07         P25p2 LCH 1  4V 1
 AMBE E35FCFFDA0FC80 err = [3] [3]
 AMBE ADF252ABBE8780 err = [2] [3]
 AMBE D7292727F3D100 err = [1] [3]
 AMBE 24B7ECFCC86500 err = [1] [3]

17:21:07         P25p2 LCH 0  R-S ERR Fs
17:21:07         P25p2 LCH 1  4V 2
 AMBE 1E10034D7F6100 err = [3] [4]
 AMBE D8490B9B85BD80 err = [2] [4]
 AMBE 51684B50153A80 err = [2] [4]
 AMBE 727A3035DE1300 err = [1] [4]

17:21:07 Sync: +P25p2 SISCH  WACN [BEE00] SYS [49A] NAC [49A]
17:21:07         P25p2 LCH 0  R-S ERR Fs
17:21:07         P25p2 LCH 1  4V 3
 AMBE 29EDA83FBE4580 err = [3] [4]
 AMBE FE8D88D76FBF80 err = [2] [4]
 AMBE E3C85488FFBE80 err = [2] [3]
 AMBE 6C8B0E44F5AE80 err = [2] [3]

17:21:07         P25p2 LCH 0  R-S ERR Fs
17:21:07         P25p2 LCH 1  4V 4
 AMBE 867544952D4880 err = [1] [2]
 AMBE E936446C1BEF80 err = [2] [4]
 AMBE 116424BC7F6A80 err = [1] [4]
 AMBE 903C6D0E231280 err = [2] [5]

17:21:07 Sync: +P25p2 SISCH  WACN [BEE00] SYS [49A] NAC [49A]
17:21:07         P25p2 SACCH  R-S ERR Ss
17:21:07         P25p2 SACCH  R-S ERR Ss
17:21:07         P25p2 LCH 0  R-S ERR Fs
17:21:07         P25p2 LCH 1  2V
 AMBE 852A45F365FA80 err = [2] [3]
 AMBE 2F904AF8B42280 err = [1] [4]
```

One or more of these codes are incorrect, so the DSD-FME decoding is incorrect.

The special thing about the P25 Phase 2 is that you need to give dsd-fme the correct WACN/ SYS and NAC codes with -X option. These codes are used to decrypt the data. If any of these codes are incorrect, the data will not be properly decrypted and there will be errors everywhere.

-X <hex> Manually Set P2 Parameters (WACN, SYSID, CC/NAC) (-X BEE00ABC123)

How do I find these codes?

These codes are broadcast on the control channel (NET_STS_BCST), so you must listen to the control channel corresponding to this voice channel to get the WACN, SYSID and CC/NAC.