

NXDN 48/96 AND dPMR KEY FINDER for RASPBERRY PI CO

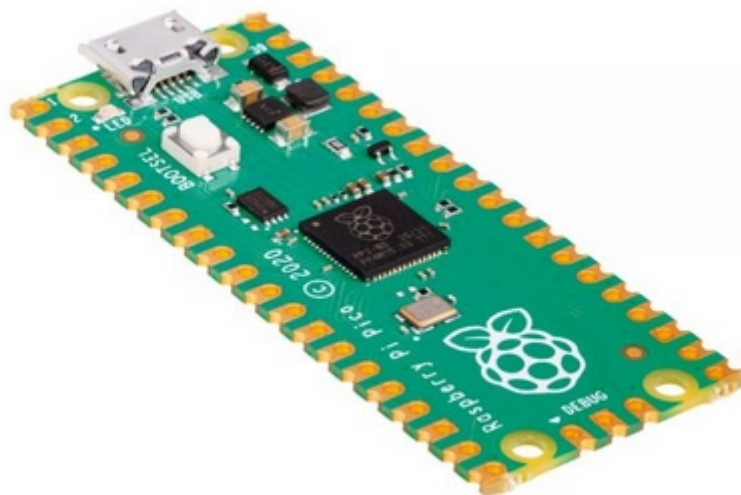
Disclaimer: This software must be used on your own radios in your test lab. Do not use this software on radios that do not belong to you, it is illegal in most countries. Check your local legislation.

This software allows you to find the key to the NXDN 48/96 and dPMR scramblers.


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

A Raspberry PICO costs about 3 dollars and looks like this:


I tested this software on a PICO W (Wifi) but normally it should work on a normal PICO.

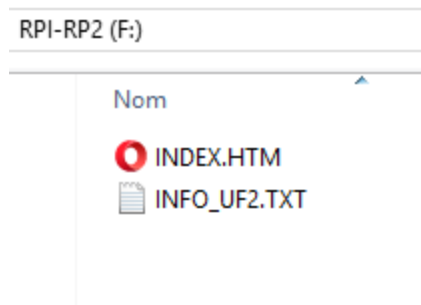


It connects to a PC using a USB cable. You will have to press the BOOTSEL button while connecting the USB socket of the PC, this opens an additional drive:

 RPI-RP2 (F:)

Copy-paste or drag-and-drop the **nxdnkeyfinder.uf2** file into the drive and you're done.

 nxdnkeyfinder.uf2



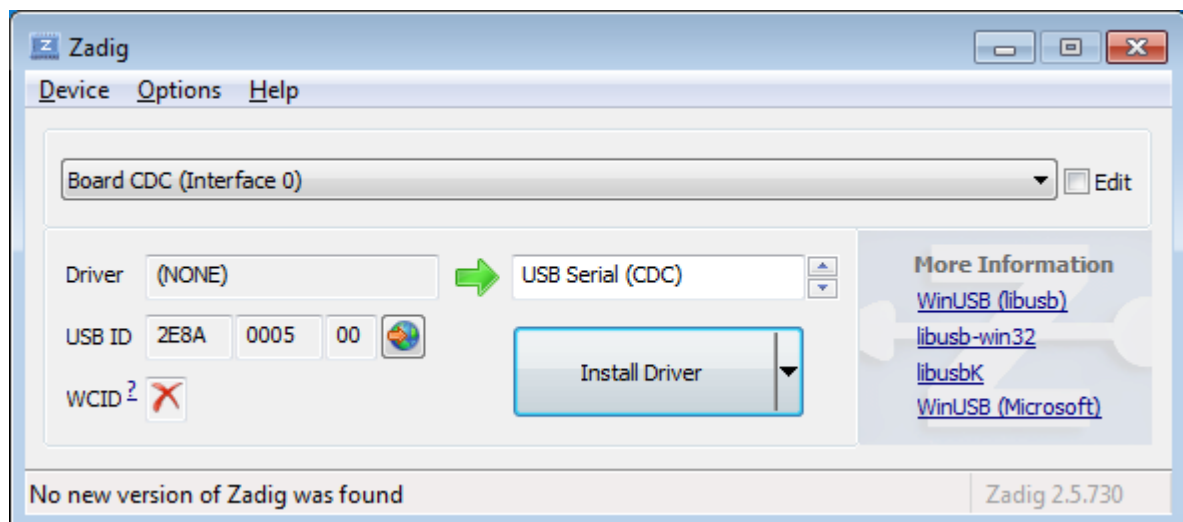
If you are using an old Windows (before Windows 10), use the Zadig software to have the additional USB port recognized.

<https://zadig.akeo.ie/>


Download and run Zadig.

Connect the Raspberry PICO to the PC.

Select Board CDC (Interface 0) from the drop-down box. Select USB Serial (CDC) as the driver.



Then click Install Driver. A serial port will be assigned when the installation is complete.

 Board CDC (Interface 0) (COM6)

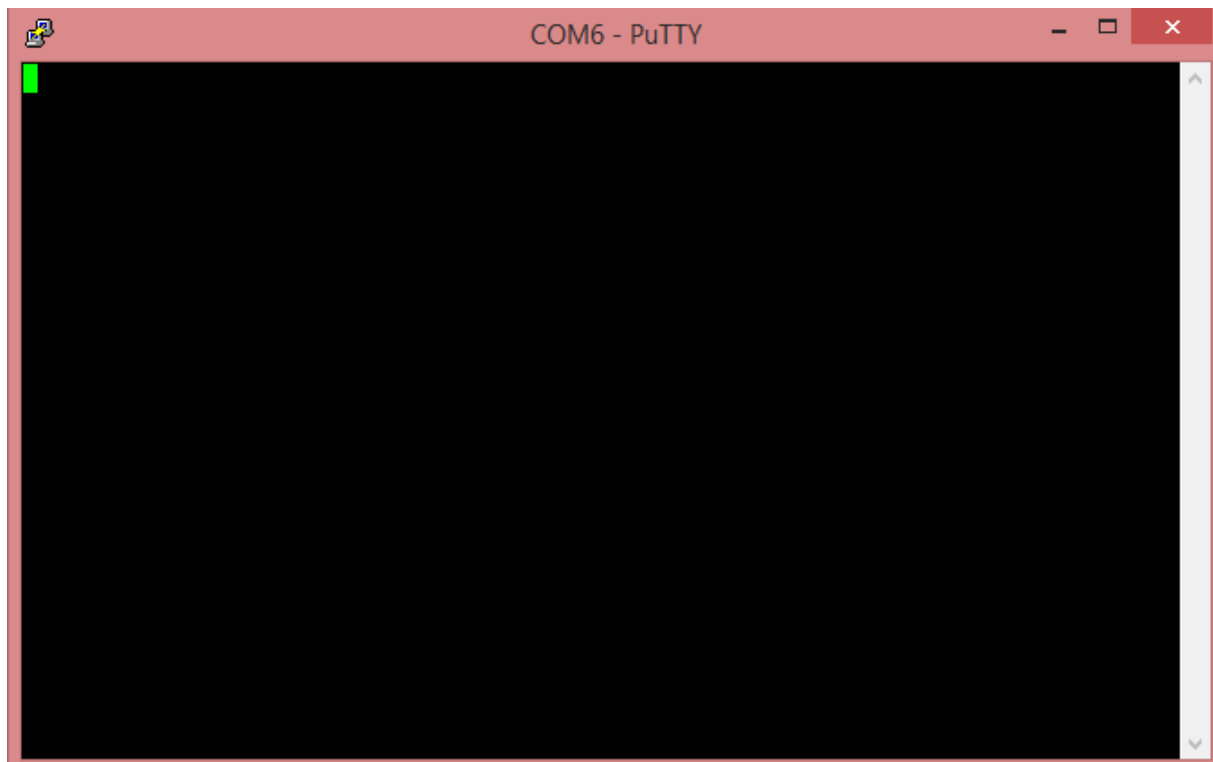
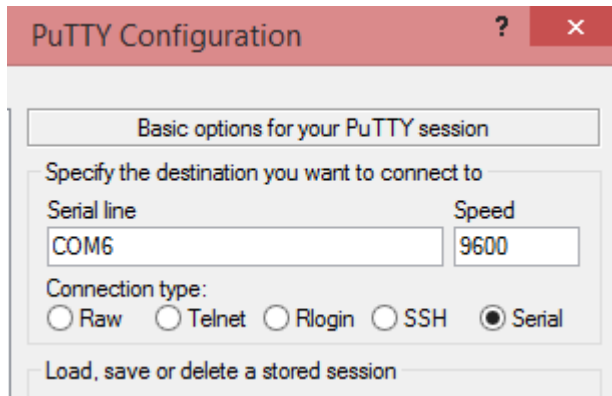
Download the Putty software for Windows and enter this (the Raspberry PICO must be connected to the PC).

Serial

COM6

speed 9600

Click **Open**



Press any key:

```
COM6 - PuTTY
NXDN & DPMR Key Finder v0.3 for Raspberry Pi PICO Awit Team (c) 2021

1-NXDN48 key finder
2-NXDN96 key finder
3-dPMR key finder

4-Quit

Your choice:
```

NXDN48:

Enter the 16 frames:

```
COM6 - PuTTY

2-NXDN96 key finder
3-dPMR key finder

4-Quit

Your choice:1

Enter AMBE Frame 1/16 :|FEBB0EE1455680|
Enter AMBE Frame 2/16 :|C0E018A223EA80|
Enter AMBE Frame 3/16 :|847EDDDDB04B910|
Enter AMBE Frame 4/16 :|077ACEDD08A280|
Enter AMBE Frame 5/16 :|1D45CD0598B300|
Enter AMBE Frame 6/16 :|447964F4FBB600|
Enter AMBE Frame 7/16 :|D52B13ED60CB80|
Enter AMBE Frame 8/16 :|73EE9D0552FB80|
Enter AMBE Frame 9/16 :|6805BF06CECD00|
Enter AMBE Frame 10/16 :|A2F9356645C800|
Enter AMBE Frame 11/16 :|DF43BBBFC5CB80|
Enter AMBE Frame 12/16 :|5AAFA11D32AD00|
Enter AMBE Frame 13/16 :|DA6FA659609D00|
Enter AMBE Frame 14/16 :|AEE2DC19F83C00|
Enter AMBE Frame 15/16 :|5A317D5AF3A680|
Enter AMBE Frame 16/16 :|636FEF3F667380|
```

```
Please wait...
```

```
Please wait...
```

```
Key found: 21347
```

```
End, press a key to restart !
```

NXDN96 :

Enter the 8 frames:

```
COM6 - PuTTY
NXDN & DPMR Key Finder v0.3 for Raspberry Pi PICO Awit Team (c) 2021

1-NXDN48 key finder
2-NXDN96 key finder
3-dPMR key finder

4-Quit

Your choice:2

Enter AMBE Frame 1/8 :|38DFEB85A18D00|
Enter AMBE Frame 2/8 :|D7DD5572C3D700|
Enter AMBE Frame 3/8 :|DB14095B1EF680|
Enter AMBE Frame 4/8 :|D50D2FA1AB3F80|
Enter AMBE Frame 5/8 :|ABA727C3B2FD80|
Enter AMBE Frame 6/8 :|B547549B49AF80|
Enter AMBE Frame 7/8 :|92D0B2473A5D00|
Enter AMBE Frame 8/8 :|3E81EA12D97E00|

Please wait...
```

```
COM6 - PuTTY
2-NXDN96 key finder
3-dPMR key finder

4-Quit

Your choice:2

Enter AMBE Frame 1/8 :|38DFEB85A18D00|
Enter AMBE Frame 2/8 :|D7DD5572C3D700|
Enter AMBE Frame 3/8 :|DB14095B1EF680|
Enter AMBE Frame 4/8 :|D50D2FA1AB3F80|
Enter AMBE Frame 5/8 :|ABA727C3B2FD80|
Enter AMBE Frame 6/8 :|B547549B49AF80|
Enter AMBE Frame 7/8 :|92D0B2473A5D00|
Enter AMBE Frame 8/8 :|3E81EA12D97E00|

Please wait...

Potential Key found: 4355
Potential Key found: 15106

End, press a key to restart !
```

How do I get NXDN or dPMR frames?

Use DSD-FME.

To get help:

`dsd-fme.exe -h`

```
-fi          Decode only NXDN48* (6.25 kHz) / IDAS*
-fn          Decode only NXDN96* (12.5 kHz)
-fp          Decode only EDACS/ProVoice*
-fm          Decode only dPMR*
```

For NXDN48:

`dsd-fme -Z -fi`

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 -fi -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 -fi -i rtl:1:432.153M:22:-2:12:0:6021 2>log.txt
```

You must use the first 16 frames of an NXDN48 transmission, but be careful, you have to start at Segment #1 (PF 1/4) then use Segment #2, then #3 and finally #4

It is necessary to ensure that the errors are at 0:

```
AMBE 3CC1708B0DC600 err = [0] [0]
AMBE 46ABCE167E6900 err = [0] [0]
AMBE 279F8ECA6A9900 err = [0] [0]
AMBE CF3C3DE16C6C80 err = [0] [0]
```

[0] [0] = no
error

```
AMBE 90D59D6744A500 err = [0] [1]
AMBE 5804AB45755D00 err = [1] [2]
AMBE 2A5DDD437AD700 err = [0] [2]
AMBE AE02015C53FF80 err = [0] [2]
```

[0][1]
[1][2] =
errors

It is not always possible to have the reception without any errors and sometimes this software even works with errors.

But if it doesn't work, then you have too many reception errors.

12:14:18 Sync: NXDN48 L40 - RDCH ESC[36m Data ESC[0m PF 1/1 IDLE
SACCH NSF [A2][DA][31][69]ESC[31m (CRC ERR)ESC[0m
FACCH1 Payload [07][8D][72][41][A2][CA][2B][8E][28][A5][7D][00]ESC[31m (CRC ERR)ESC[0m
FACCH1 Payload [62][5C][DB][E8][A5][D2][8D][40][1C][CB][1C][90]ESC[31m (CRC ERR)ESC[0m
Lich Parity Error 69

false sync or unsupported NXDN lich type 0x58

Lich Parity Error 02

12:14:18 Sync: NXDN48 L57 - RDCH ESC[32m Voice ESC[0mESC[36m ESC[0mPF 3/4

SACCH SF Segment #3 [49][90][00][1D]

AMBE 90D59D6744A500 err = [0] [1]

AMBE 5804AB45755D00 err = [1] [2]

AMBE 2A5DDD437AD700 err = [0] [2]

AMBE AE02015C53FF80 err = [0] [2]

12:14:18 Sync: NXDN48 L57 - RDCH ESC[32m Voice ESC[0mESC[36m RAN 09 ESC[0mPF 4/4

Full SACCH Payload [FF][FF][FF][FF][F9][00][00][56][00]

SACCH SF Segment #4 [09][15][80][14]

AMBE 3CC1708B0DC600 err = [0] [0]

AMBE 46ABCE167E6900 err = [0] [0]

AMBE 279F8ECA6A9900 err = [0] [0]

AMBE CF3C3DE16C6C80 err = [0] [0]

12:14:18 Sync: NXDN48 L57 - RDCH ESC[32m Voice ESC[0mESC[36m RAN 09 ESC[0mPF 1/4

SACCH SF Segment #1 [C9][3F][68][81]

AMBE FEBB0EE1455680 err = [0] [0]

AMBE C0E018A223EA80 err = [0] [0]

AMBE 847EDDB04B9100 err = [0] [0]

AMBE 077ACEDD08A280 err = [0] [0]

12:14:18 Sync: NXDN48 L57 - RDCH ESC[32m Voice ESC[0mESC[36m RAN 09 ESC[0mPF 2/4

SACCH SF Segment #2 [89][08][10][B6]

AMBE 1D45CD0598B300 err = [0] [0]

AMBE 447964F4FBB600 err = [0] [0]

AMBE D52B13ED60CB80 err = [0] [0]

AMBE 73EE9D0552FB80 err = [0] [0]

12:14:18 Sync: NXDN48 L57 - RDCH ESC[32m Voice ESC[0mESC[36m RAN 09 ESC[0mPF 3/4

SACCH SF Segment #3 [49][40][00][2D]

AMBE 6805BF06CECD00 err = [0] [0]

AMBE A2F9356645C800 err = [0] [0]

AMBE DF43BBBFC5CB80 err = [0] [0]

AMBE 5AAFA11D32AD00 err = [0] [0]

18:19:53 Sync: NXDN48 L57 - RDCH ESC[32m Voice ESC[0mESC[36m RAN 09 ESC[0mPF 4/4ESC[33m ALIASESC[0m

Full SACCH Payload [3F][68][82][04][24][00][00][00][00]

SACCH SF Segment #4 [09][00][00][15]

AMBE DA6FA659609D00 err = [0] [1]

AMBE AEE2DC19F83C00 err = [0] [2]

AMBE 5A317D5AF3A680 err = [2] [0]

AMBE 636FEF3F667380 err = [0] [0]

18:19:53 Sync: NXDN48 L57 - RDCH ESC[32m Voice ESC[0mESC[36m RAN 09 ESC[0mPF 2/4

Too many reception errors

First Segment 1/4

[0][0] good no errors

There are errors but we try anyway, sometimes it works

For NXDN96:

`dsd-fme -Z -fn`

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 -fn -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 -fi -i rtl:1:432.153M:22:-2:12:0:6021 2>log.txt`

You must use the first 8 frames of an NXDN48 transmission, but be careful, you have to start at Segment #1 (PF 1/4) and then use Segment #3 (PF 3/4) because segments #2 and #4 do not exist in Half Duplex.

Sometimes you can start further, not just at the very beginning of the transmission but there is less chance that it will work or you can find several potential keys instead of just one.

For example, here, we have to start much lower, because there are too many reception errors:

Segment
1/4 not
usable

```
18:24:32 Sync: NXDN96 L51 - RDCH ESC[36m Data ESC[0mESC[36m RAN 24 ESC[0mPF 1/4
SACCH SF Segment #1 [D8][01][00][08]ESC[33m ALIASESC[0m INTE
FACCH1 Payload [3F][68][82][04][14][49][4E][54][45][00][33][E0]
FACCH1 Payload [3F][46][E9][5A][4F][96][90][06][E3][2F][8D][30]ESC[31m (CRC ERR)ESC[0m
18:24:32 Sync: NXDN96 L51 - RDCH ESC[36m Data ESC[0mESC[36m RAN 24 ESC[0mPF 2/4
SACCH SF Segment #2 [98][88][0C][A4]
FACCH1 Payload [3F][68][82][04][34][20][1D][C1][9D][1A][4F][80]ESC[31m (CRC ERR)ESC[0mESC[33m ALIASESC[
FACCH1 Payload [3F][68][82][04][44][00][00][03][1B][00][CB][70]
18:24:32 Sync: NXDN96 L57 - RDCH ESC[32m Voice ESC[0mESC[36m RAN 24 ESC[0mPF 3/4
SACCH SF Segment #3 [58][20][02][D7]
AMBE 8BBF90C1B2F380 err = [0] [0]
AMBE 9589BE2599EF00 err = [0] [0]
AMBE 26961E3594DA80 err = [0] [1]
AMBE 3CA62295BF0E00 err = [0] [1]
18:24:32 Sync: NXDN96 L51 - RDCH ESC[36m Data ESC[0mESC[36m RAN 24 ESC[0mPF 4/4ESC[33m VCALLESC[0mESC
Group Call - Half Duplex 9600bps/EHR (02) - Src=802 - Dst/TG=44 ESC[0m
ESC[33mScrambler - Key ID 0 - ESC[0m
Full SACCH Payload [01][00][22][03][22][00][2C][40][00]
SACCH SF Segment #4 [18][10][00][29]ESC[33m VCALLESC[0mESC[32m
Group Call - Half Duplex 9600bps/EHR (02) - Src=802 - Dst/TG=44 ESC[0m
ESC[33mScrambler - Key ID 0 - ESC[0m
FACCH1 Payload [01][00][22][03][22][00][2C][40][00][00][30][20]
FACCH1 Payload [01][00][22][01][D3][35][CC][40][00][00][30][20]ESC[31m (CRC ERR)ESC[0m
18:24:32 Sync: NXDN96 L57 - RDCH ESC[32m Voice ESC[0mESC[36m RAN 24 ESC[0mPF 1/4
SACCH SF Segment #1 [D8][3F][68][AB]
AMBE A8DF36D2A93D00 err = [0] [0]
AMBE A7CB19FBC4EE80 err = [0] [1]
AMBE FB14B33ADAF000 err = [1] [1]
AMBE F50DED07E33680 err = [0] [0]
18:24:32 Sync: NXDN96 L51 - RDCH ESC[36m Data ESC[0mESC[36m RAN 24 ESC[0mPF 2/4
SACCH SF Segment #2 [98][08][10][52]
FACCH1 Payload [01][D7][44][A0][69][71][8A][50][02][8D][6E][20]ESC[31m (CRC ERR)ESC[0m
FACCH1 Payload [34][40][05][BB][F3][28][07][29][6D][75][8B][E0]ESC[31m (CRC ERR)ESC[0m
Lich Parity Error 73
Lich Parity Error 62
18:24:32 Sync: NXDN96 L51 - RDCH ESC[36m Data ESC[0mESC[36m RAN 24 ESC[0mPF 4/4
Full SACCH Payload [3F][68][82][04][1F][FF][FC][1F][24]
SACCH SF Segment #4 [18][07][C9][1C] CRC ERR - 0E 1C
FACCH1 Payload [01][00][00][68][B8][D7][3E][2B][8D][1A][5B][E0]ESC[31m (CRC ERR)ESC[0m
FACCH1 Payload [01][00][22][01][D3][23][54][40][00][00][30][60]ESC[31m (CRC ERR)ESC[0m
18:24:32 Sync: NXDN96 L57 - RDCH ESC[32m Voice ESC[0mESC[36m RAN 24 ESC[0mPF 1/4
SACCH SF Segment #1 [D8][3F][68][AB]
AMBE 38DFEB85A18D00 err = [0] [1]
AMBE D7DD5572C3D700 err = [0] [1]
AMBE DB14095B1EF680 err = [1] [1]
AMBE D50D2FA1AB3F80 err = [0] [0]
```

Segment
3/4 does
not appear

Ok Segment
1/4 usable

```
14:19:40 Sync: NXDN96 L51 - RDCH ESC[36m Data ESC[0mESC[36m RAN 24 ESC[0mPF 2/4
SACCH SF Segment #2 [98][08][10][9C]ESC[33m VCALLESC[0mESC[32m
Group Call - Half Duplex 9600bps/EHR (02) - Src=802 - Dst/TG=44 ESC[0m
ESC[33mScrambler - Key ID 0 - ESC[0m
FACCH1 Payload [01][00][22][03][22][00][2C][40][00][00][30][20]
FACCH1 Payload [01][00][22][01][D0][6B][8A][F8][D7][1A][5B][E0]ESC[31m (CRC ERR)ESC[0m
14:19:40 Sync: NXDN96 L57 - RDCH ESC[32m Voice ESC[0mESC[36m RAN 24 ESC[0mPF 3/4
SACCH SF Segment #3 [58][45][24][0B]
AMBE ABA727C3B2FD80 err = [0] [1]
AMBE B547549B49AF80 err = [0] [0]
AMBE 92D0B2473A5D00 err = [0] [1]
AMBE 3E81EA12D97E00 err = [0] [1]
```

Ok Segment 3/4
usable

There are errors but
we try anyway,
sometimes it works