# WD 2.1.7.x Firmware Unlocking Tutorial Full Version

目录

Preface.....1
Section Ⅰ WD Firmware Unlock Preparation.....2
Section Ⅱ Connection of The Programmer.....3
Section Ⅲ The Use of Programmer.....4
Section Ⅳ Terminal Connection.....11
Section Ⅴ Unlocking the Firmware.....14

## Preface

Believe that WD 800xx hard drives of and above series have always brought considerable trouble to everyone. For example, the purchase of an unlocked board requires additional cost. The price of some unlocked boards is also quite high for certain PCB versions. In addition ,there may be two versions of a few unlocked boards. Sometimes reading and writing ROM may cause circuit failure and PCB damage, thereby further increasing recovery cost.

Except that the existence of the firmware lock brings trouble to repair, the new series of hard drives still have data encryption problems. After converting into non-original board, data will be often encrypted.

The latest MRT version 2.7.1.x has officially released a significant new feature——WD Firmware Unlock. Currently the SATA board numbers MRT covers in new update are 800065, 800066, 800077, 810011. Its biggest advantage is that WD firmware lock can be unlocked by using the original board. There is no need to change the board.

## Section Ⅰ WD Firmware Unlock Preparation

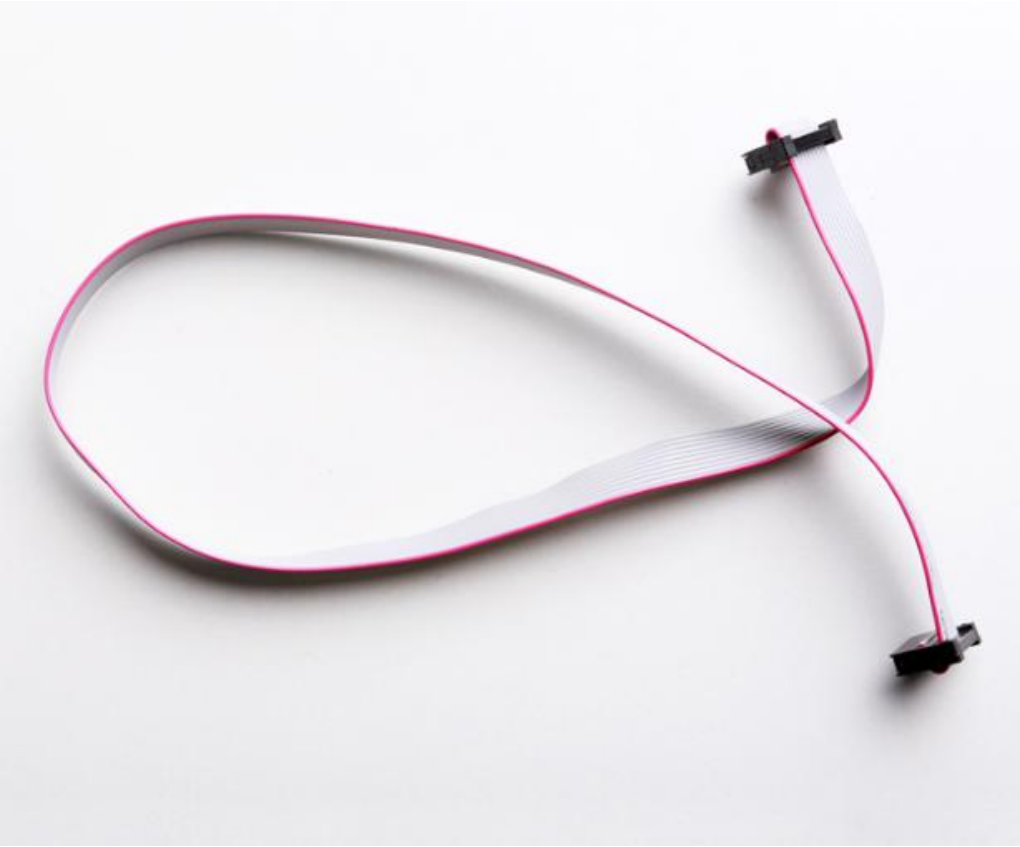
Three conditions are required for unlocking WD firmware in MRT program:

1. Original PCB board
2. Programmer (recommend MRT Programmer 3.0. Speed, stability and convenience are greatly improved).
3. Terminal adapter (must choose WD connector)

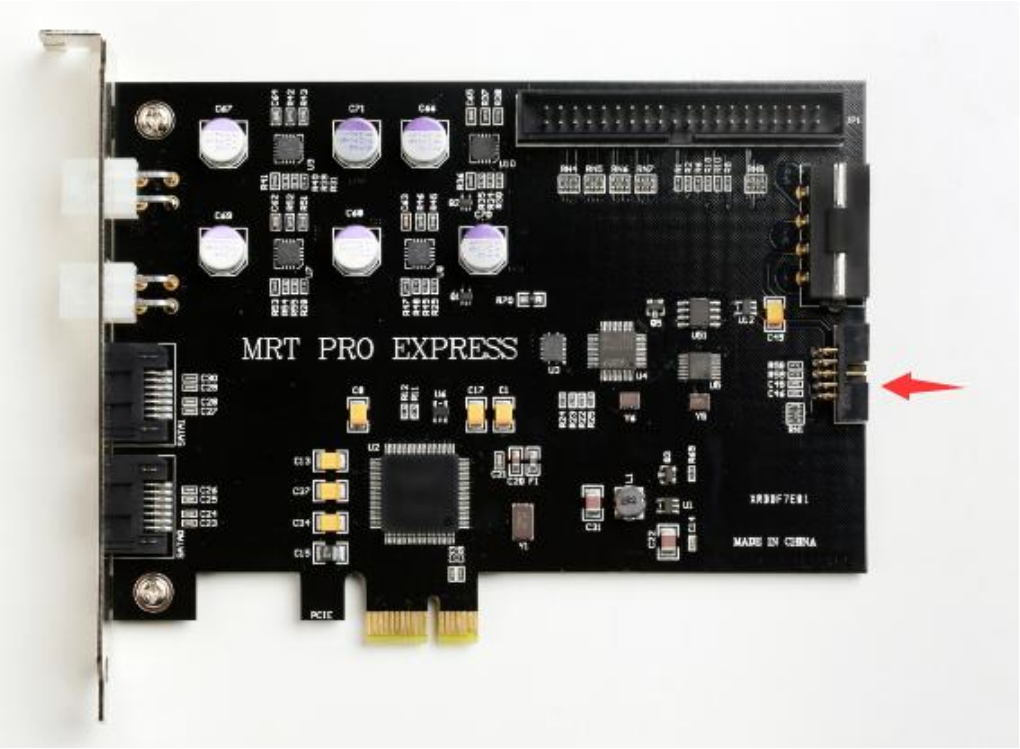
The original PCB board is a prerequisite for the application of firmware unlocking. Quite a lot of new series of hard disk converting or replacing PCB will cause data encryption. To ensure data recovery, please use the original board for unlocking.

MRT will release a new programmer in near future, namely MRT programmer 3.0. The biggest feature of this programmer is the addition of ROM pins. To realize the purpose of direct connection between programmer and ROM pins, deep adaptation has been accomplished for WD's ROM chips. Stability and compatibility of the new programmer are better than last generation. MRT programmer 3.0 can achieve the goal of reading ROM data by desoldering chip ROM or flying line method to connect ROM chip pins to programmer 3.0 pins.

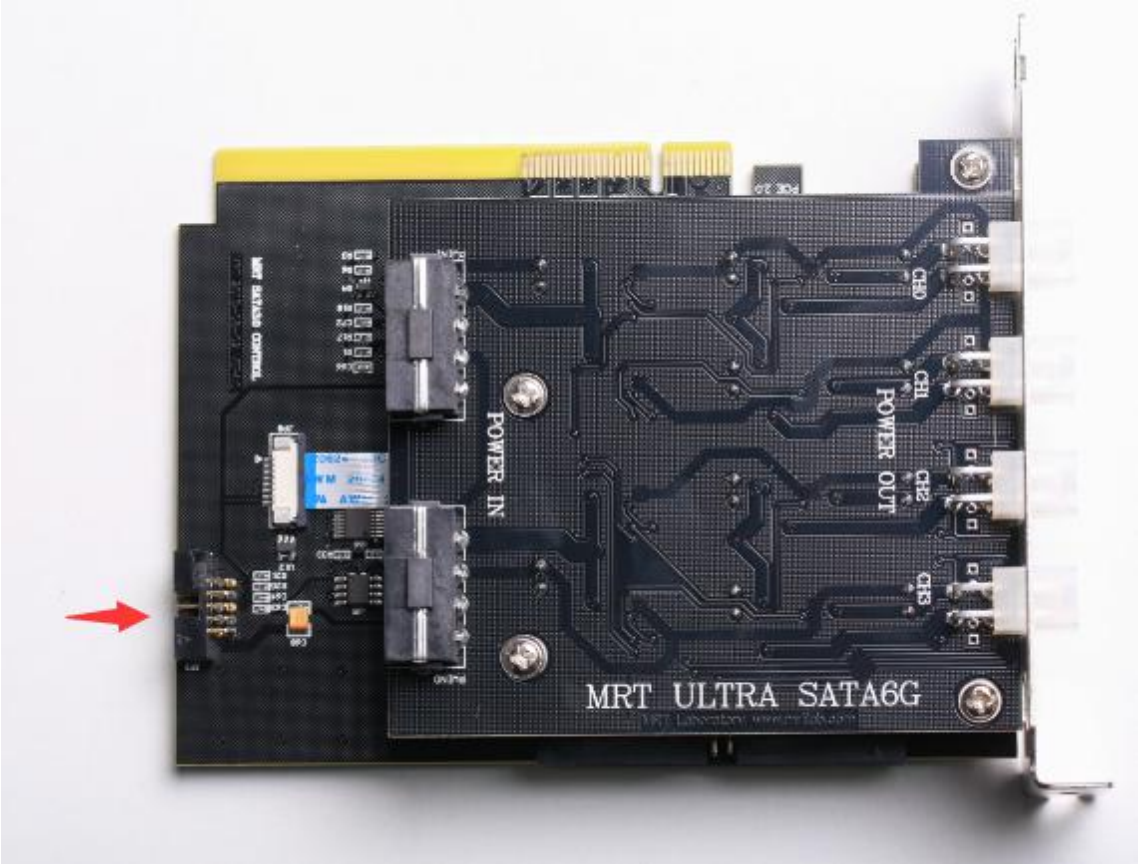
## Section Ⅱ Connection of The Programmer



Programmer cable




MRT Express programmer interface




MRT Ultra programmer interface

When connecting the programmer cable to the hardware card, please confirm the direction of the interface in advance.MRT programmer cable has a boss when designing, which is convenient to align the corresponding interface of the hardware card.

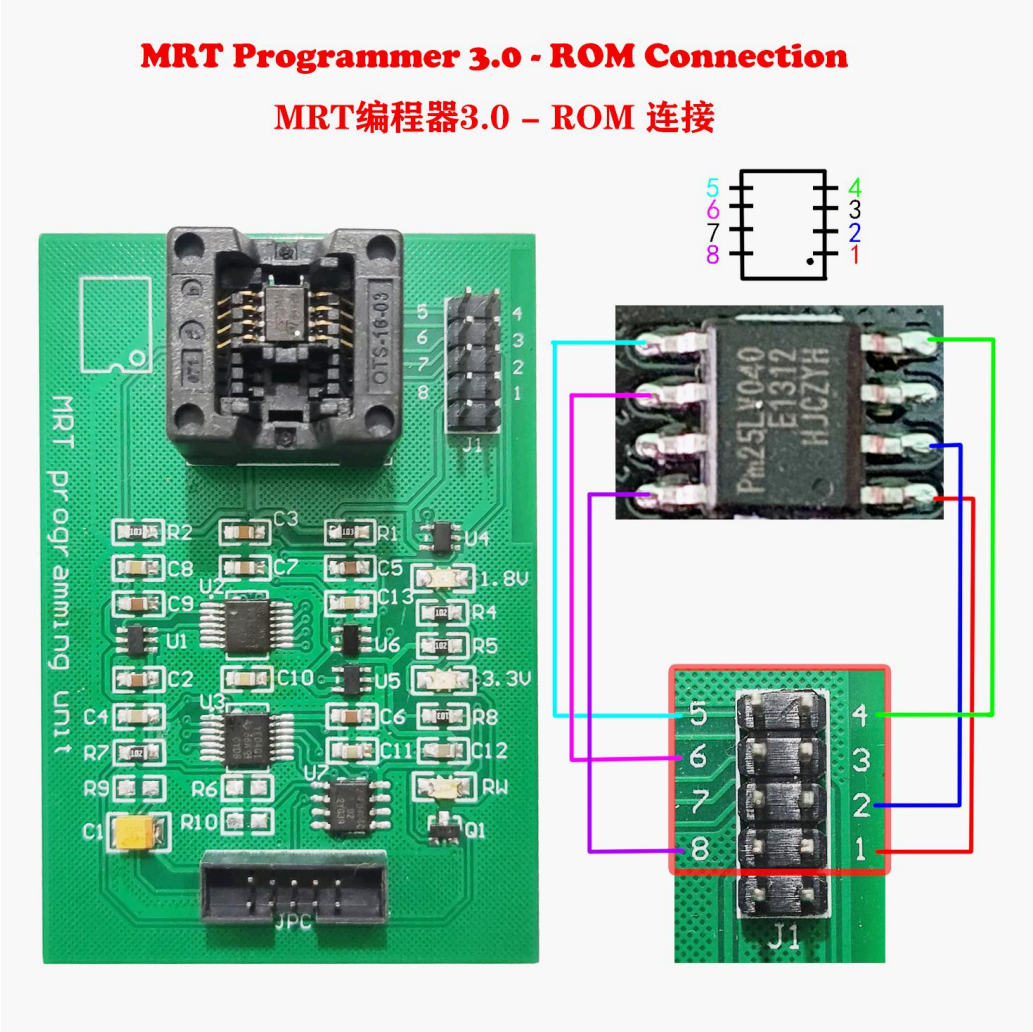
Try to hold on to the programmer interface of the hardware card to prevent the interface from loosening.Some users feed back that the hardware is stuck after connecting the programmer cable and reports "device initialization failed". Generally, it is because the port is loose or the programmer cable is not connected properly.

## Section Ⅲ The Use of Programmer

The picture below shows eight pin numbers of WD ROM chip and MRT programmer 3.0 pin numbers. The numbers are consistent.

Notice: There is a schematic diagram of the programmer at the top right of the

picture. The black dot in the lower right corner represents ROM starting pin. The direction shown in the figure is that of the programmer on the left ROM chip placement direction, that is, the small dot should face to the center of the programmer.

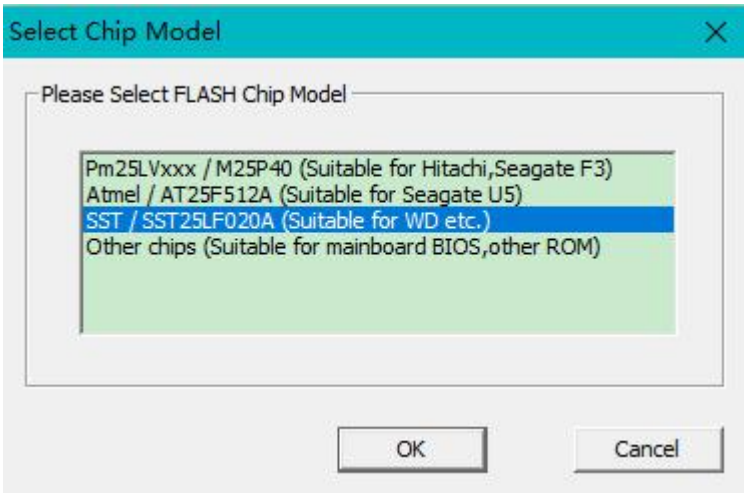


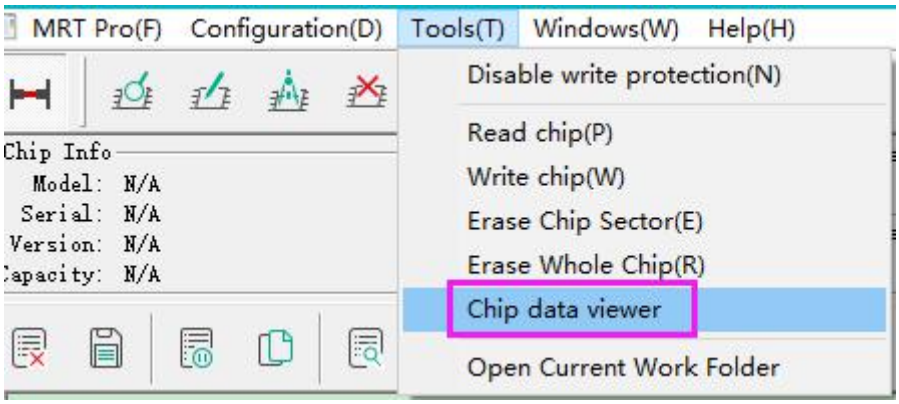

Programmer and ROM pin number

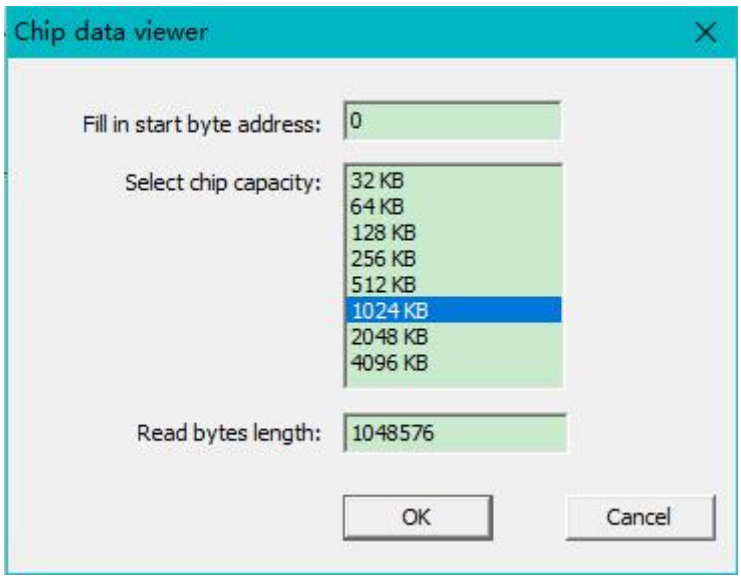
There are two methods of using MRT programmer 3.0 to read/write ROM：

1. **Conventional method:** desoldering ROM chip. Remove ROM chip and put it on programmer. After we keep the ROM backup, we can unlock ROM in WD ROM tool. WD program will generate unlock original ROM and automatically write to the chip. Then we solder ROM chip back to PCB. This method is applicable to all disks, including USB drives.

Operation path: General functions of the main interface - ROM programmer tool -Choose WD ROM item - Tools - Chip data viewer, as shown：



Common ROM size 800xx board number：

800022/41 - 512 KB

800065/67 - 1024KB

800066/69 - 1024KB

800077 - 1024KB

810011 - 1024KB

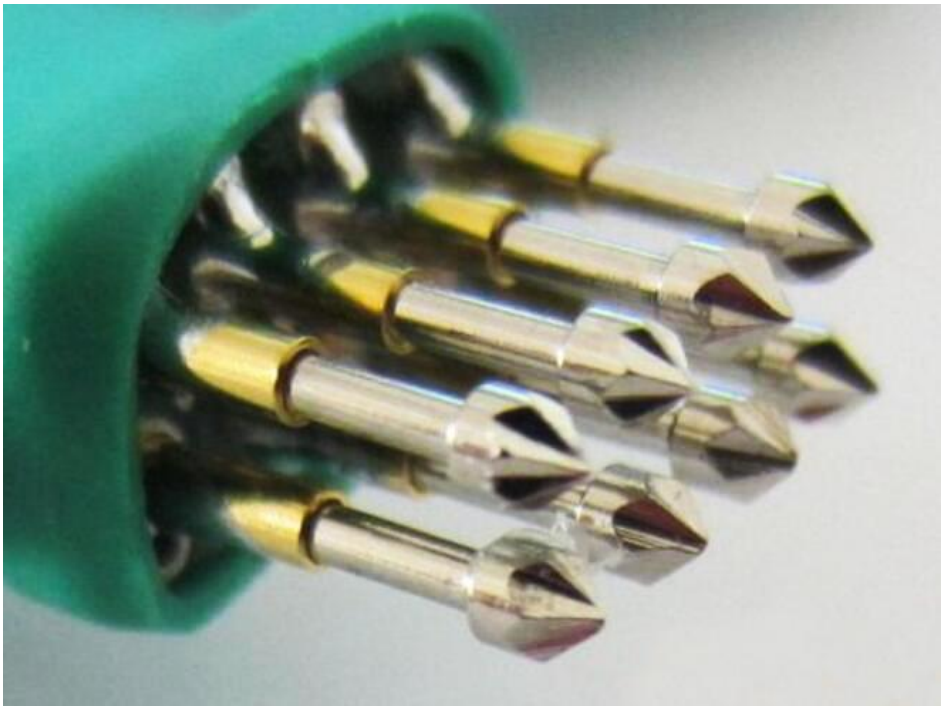
810035 - 512KB

After choosing the size, back up the original ROM. Then you can unlock the ROM in the program.

2. **Direct ROM connection method**：Connect the pins of the programmer to ROM pins.ROM pins on PCB have two kinds, namely the front and the back pins. That is, the front side displays 8 pins of the ROM chip, corresponding contacts on the back of PCB.

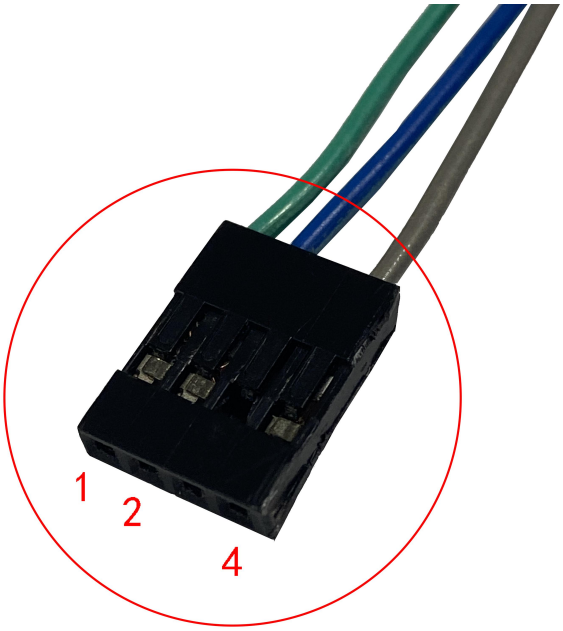
Direct connection method needs to look for the number. Figure “Programmer and ROM Pin number” shows number 1-8. The numbering sequence is in “U” type arrangement. When connected,we need exclude number 3 And number 7 Pin.

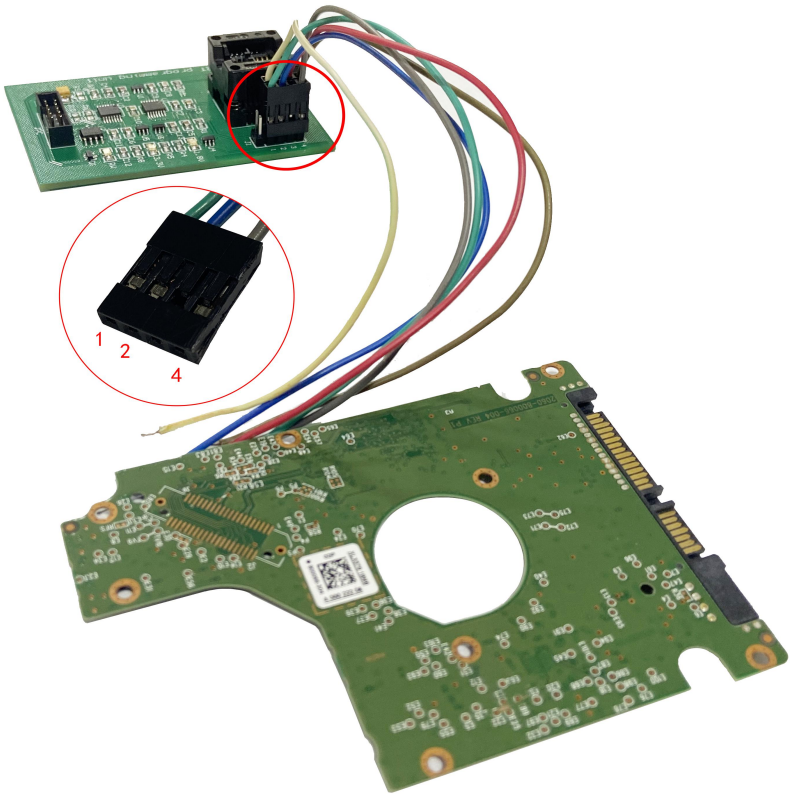
① Direct connection method of connecting programmer to ROM pins. This method requires removal of PCB and is applicable to the connection shown in the figure “Programmer and ROM pin number”. We Need to remove PCB and use the wires to connect the programmer pins to **ROM Eight Feet**. If there are proper ROM burning probe lines, connecting the programmer pins to ROM Eight Feet will be more convenient to read and write ROM, and will eliminate the welding process, as shown：



② Direct connection method of non-dismantling of PCB or ROM chip. The method needs to find related ROM pins on the back of PCB. Then connect by flying line method. Certainly, this method is relatively troublesome. It needs to weld 6 pins. Some pins have smaller vacancies. Besides, there are certain requirements for welding technology. We will study this plan further. There may be better alternatives in the future.

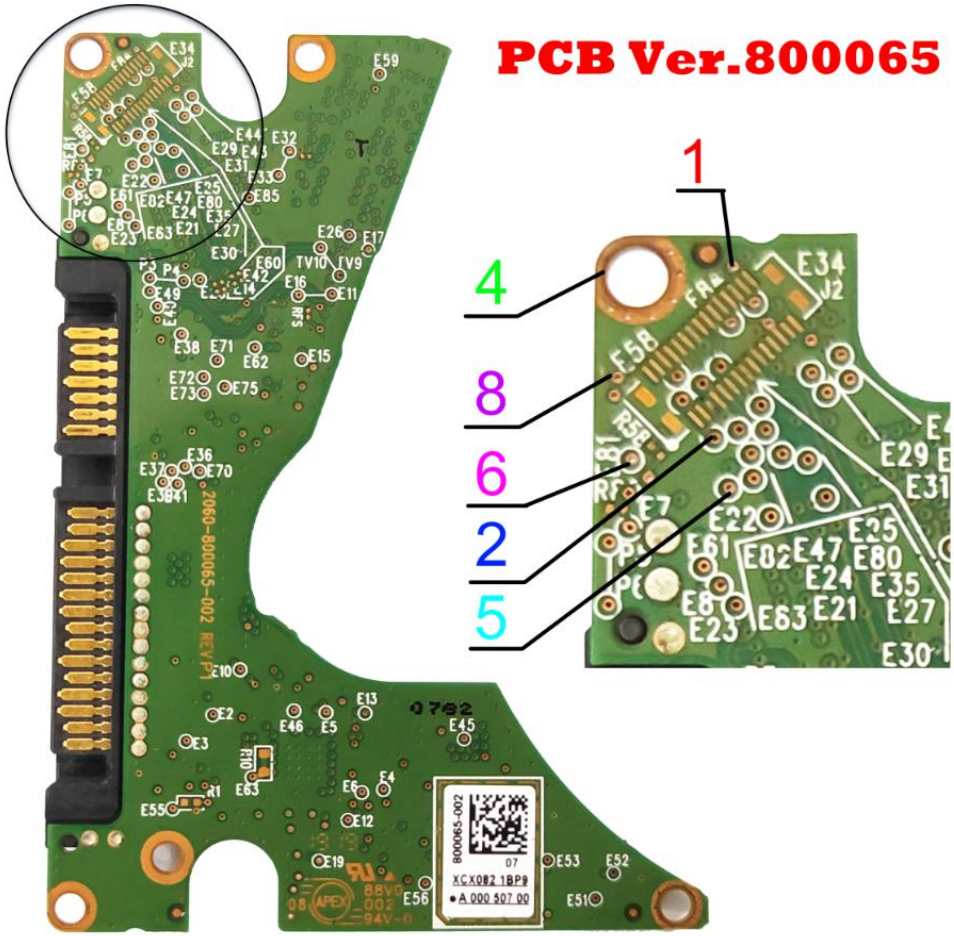
Here is a reference,for example PC motherboard jumper line, as shown below：

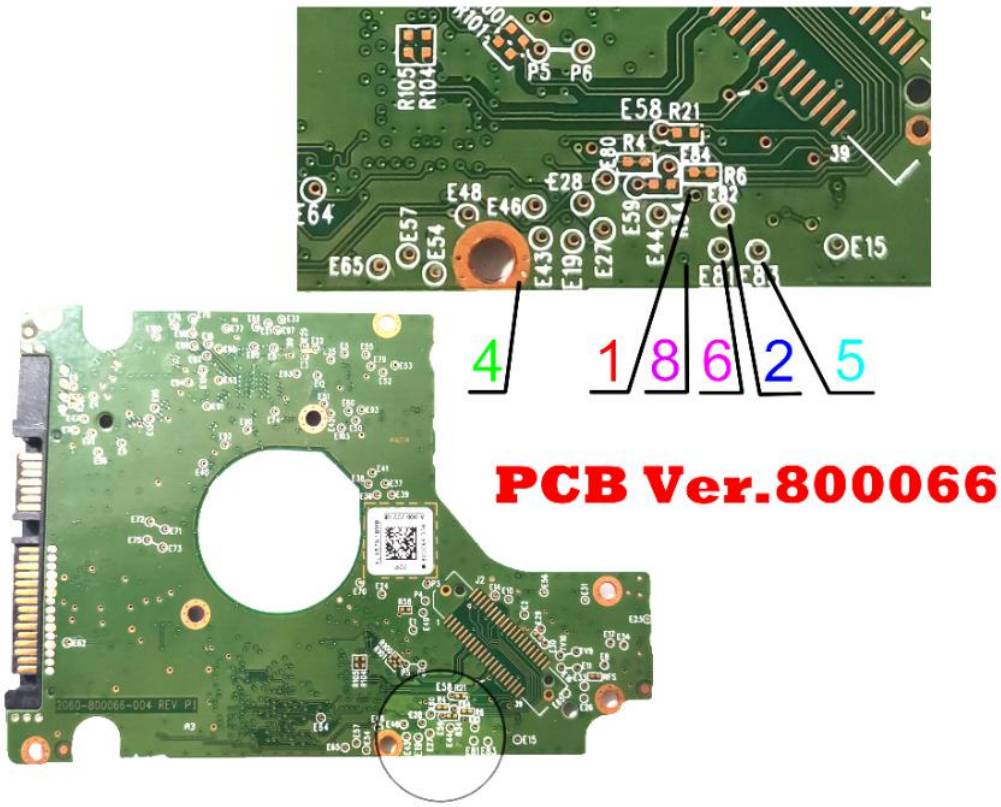


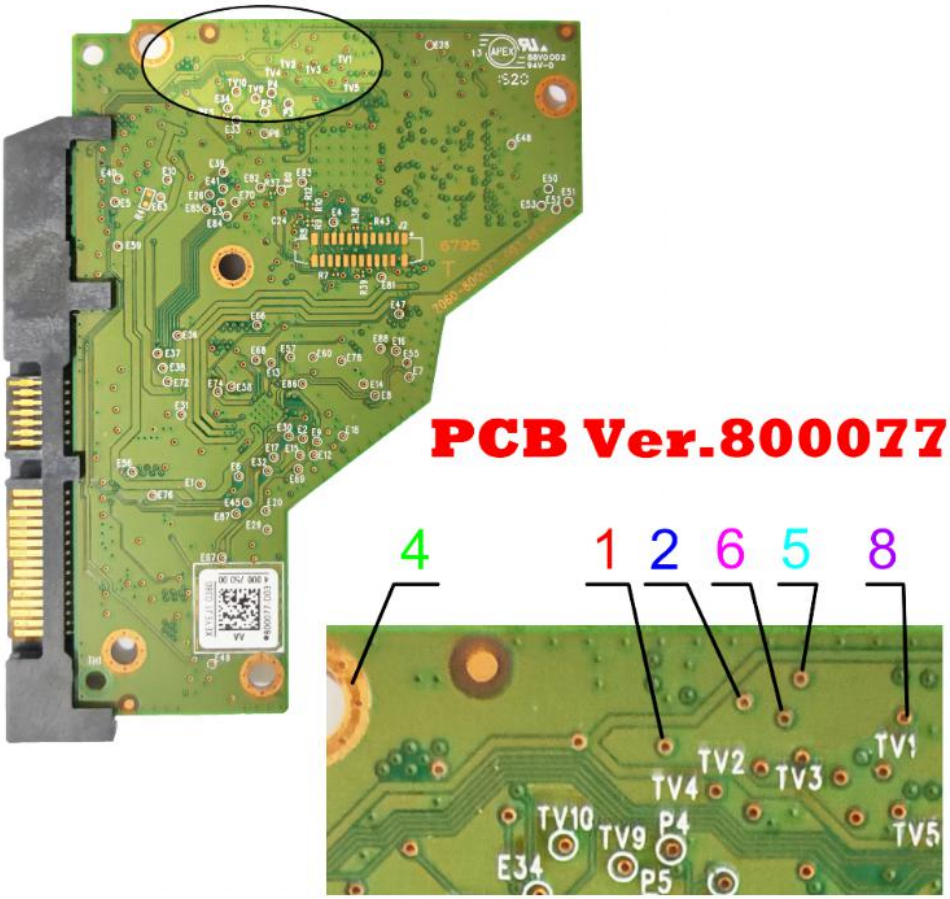




Non-dismantling of PCB or ROM of direct connection method

If you adopt this method, you need to use flying line according to PCB number, as shown below：


PCB Ver.800065
1
4
8
6
2
5

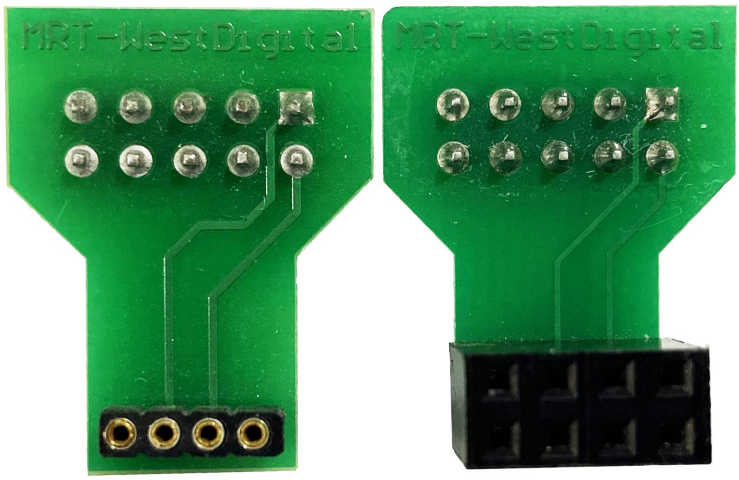

4
1
8
6
2
5
PCB Ver.800066




## Section Ⅳ Terminal Connection

Please use MRT terminal products to connect. In addition，users should select WD connectors.

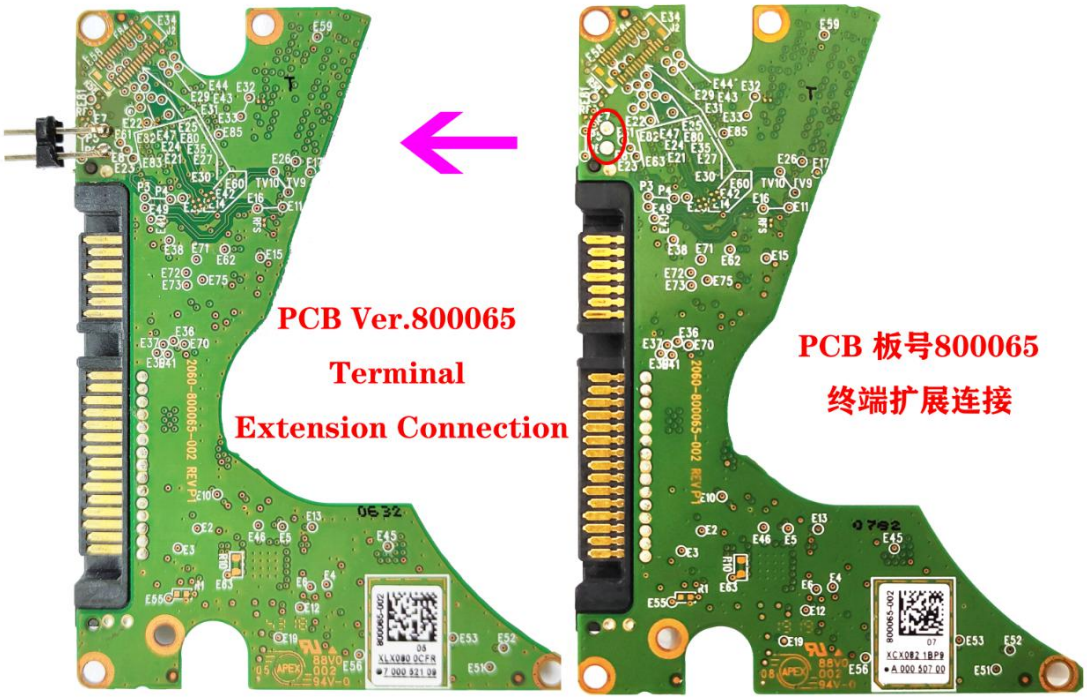
One set of MRT connectors provide a total of eight. For WD drives there are two, one for 2.5 inch hard drive and one for 3.5 inch hard drive as below：

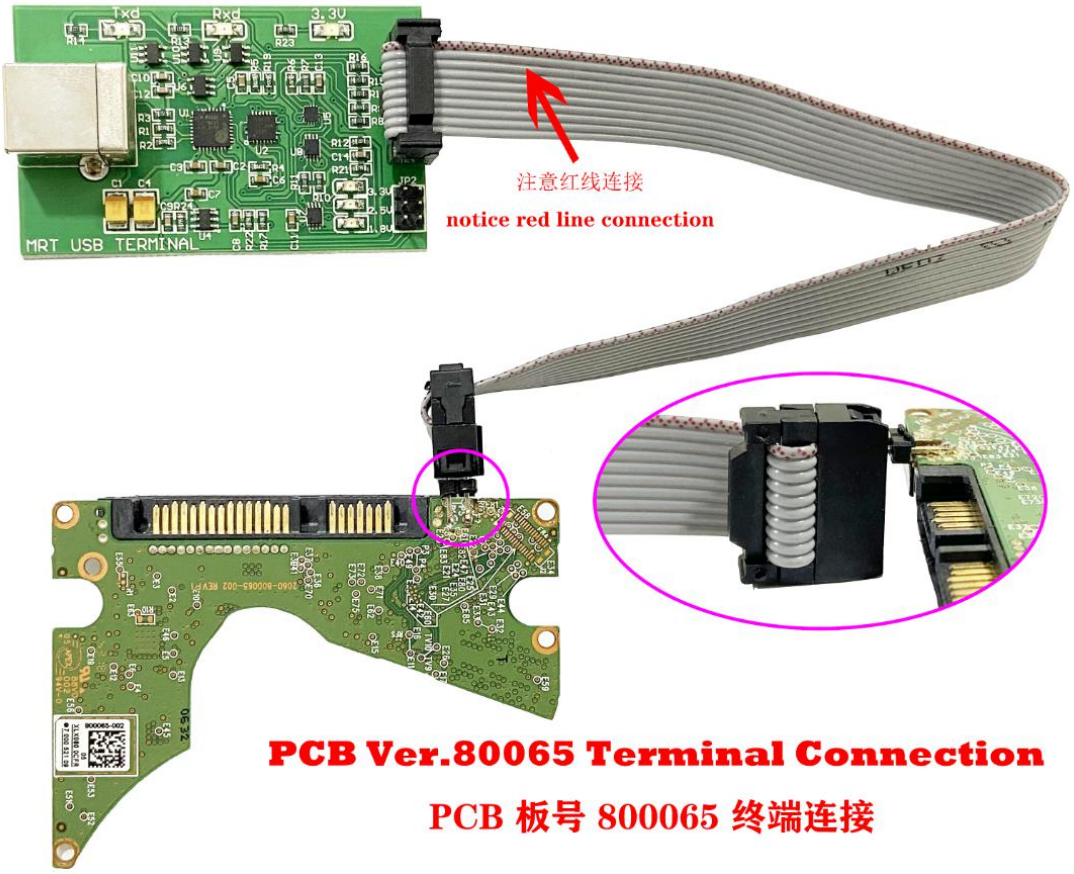



**WD Connectors**
**WD 指令头**

Terminal connection exception：serial port of PCB Ver. 800065 is very narrow so that we can't connect as normal. We can extend it by expanding the contacts. By this method we can use directly COM cable without WD connector.

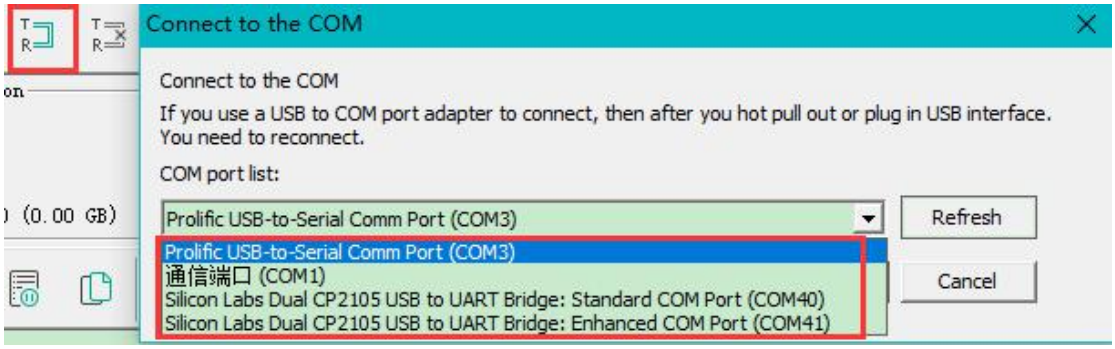
As to the same situation, if there is a similar situation with a new board number in the future, we can refer to the figure below to connect：


PCB Ver.800065
Terminal
Extension Connection
PCB 板号800065
终端扩展连接


MRT USB TERMINAL
注意红线连接
notice red line connection
PCB Ver.80065 Terminal Connection
PCB 板号 800065 终端连接

**COM port selection on software interface ：**

Click the interface button “serial port connection”, the pop-up dialog box provides COM port to be selected, as shown below：

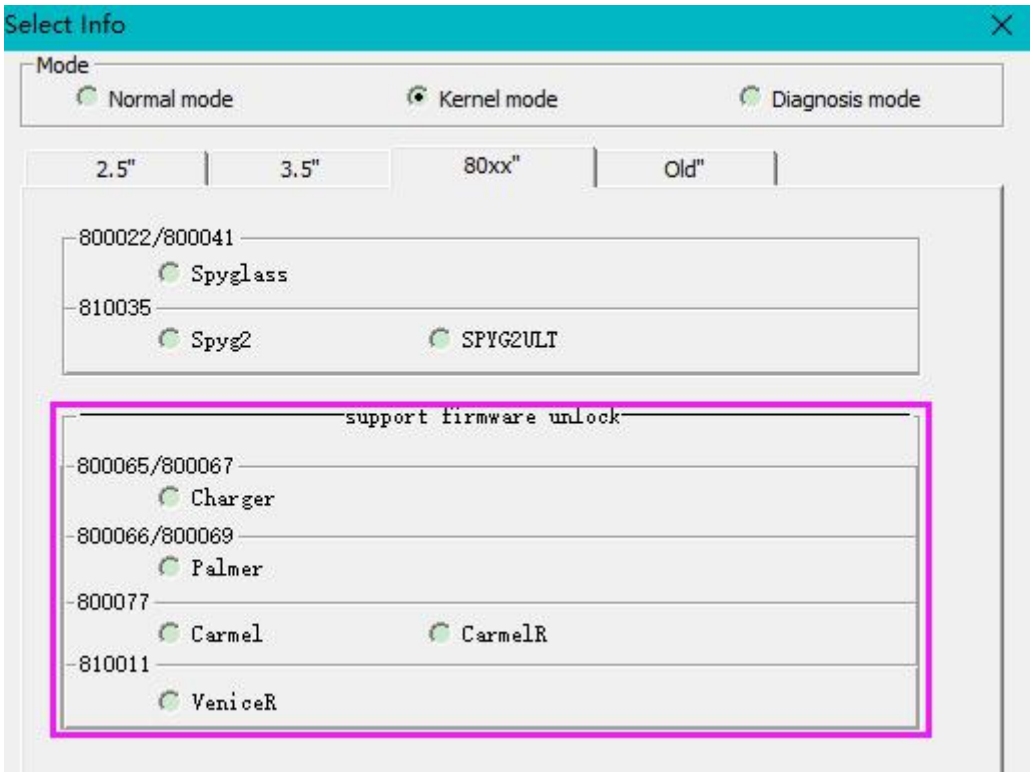



Prolific USB-to-Serial Com Port(COM 5)：New terminal（PL2303）

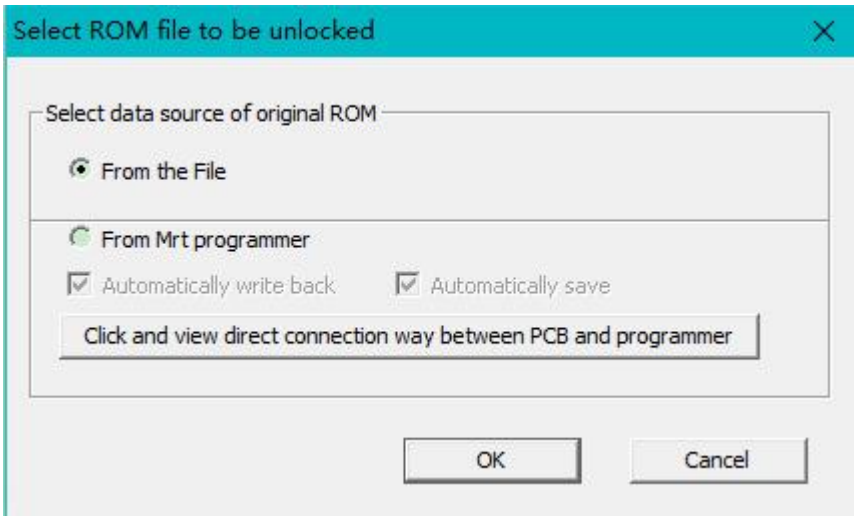
Silicon Labs Dual CP2105 USB(COM38/39)：Dual-core terminal（CP210x）

## Section Ⅴ Unlocking the Firmware

1. Manually select a family on the family panel. Since there is a firmware lock, family is accessible. We can choose the family according to the summarized board number. Since the same board number can have multiple families, without knowing the family, you can manually select any one for testing.




2. path：ROM operation button - Create unlocked ROM.




If original ROM file is saved in advance,for example previously backed up by unlocked board or desoldering the chip ROM, we choose “from the file”. After unlocking, you need to manually write unlocked ROM via programmer to ROM chip.

Notice：Be sure to use the original ROM！

If adopting desoldering method of ROM chip or flying line method, we choose

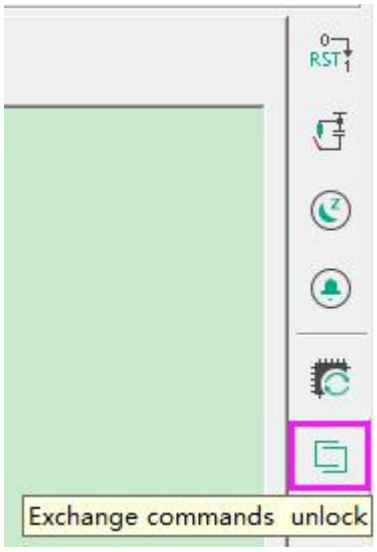
“From Mrt programmer” to get ROM source for online reading and writing ROM. At this time, it will be automatically write unlocked ROM to ROM chip via programmer.

After success as shown below, software will automatically generate a new ROM file “RomFile_Unlocked.bin”：

```
Creating unlocked ROM...
Data source of original ROM file : .............From the File
Path of original ROM file: G:\UserDataFile\WDC Marvell\Carmelr\WDC WD20EZAZ-00GGJB0-80.00A80-WD-WXU1A89EE7ZV-000200AP\SABackup\ROM\ROM_WDC WD20EZAZ-00GGJB0.bin
Path of unlocked ROM file: G:\UserDataFile\WDC Marvell\Carmelr\WDC WD20EZAZ-00GGJB0-80.00A80-WD-WXU1A89EE7ZV-000200AP\SABackup\ROM\RomFile_Unclocked.bin
Create unlocked ROM : ........................:Success
```

3. Power off and on drive. Before the first handshake(= exchange commands & unlock), it will display on the terminal interface “hello mrt!”. It means unlocked ROM has already worked, and requests a handshake to complete the final unlocking step. We can click the button “exchange commands & unlock" on the right of interface:

```
It is already in unlocking mode, please perform the unlocking function.
hello mrt!>>>
```




4.When we keep the program open,after resetting power, software will automatically exchange commands and unlock the hard disk without any manual clicking any more.

```
Exchanging commands and unlocking
Exchange commands & unlock : ....................:Success
```

5.When we exit the program, unlocked ROM applied to hard drive will show busy status each time we power on drive,which is the same as Seagate unlocking mechanism. At this point we need to manually enter WD application, click “exchange command & unlock” on family panel to make it ready. After that, disk firmware can be accessed normally.

**Notes on data encryption：**

From the results of the collection,the new generation of 800xx series has adjusted PCB number and firmware structure many times, including SED lock, firmware lock, data encryption, intensive change of board numbers, etc.. Its performance is extremely complex：

Such as USB - SATA, or locked SATA - unlocked SATA. There are situations that have data encryption and do not have data encryption. And there were a small part of models in the early days that does not have data encryption behavior after converting USB into unlocked SATA board. Another small part just follows the past strategy of data decryption like USB board 1961. We only need close SED lock and decrypt data as usual in old USB series.

Regarding the cause of encryption, i guess most of your guys have figured out that the main algorithm is in the main controller code,which leads to that current analytical tools are very limited. Therefore, data encryption issue can only be handled by flying wires so far. But the flying line also has its limitations, for example, the firmware cannot be accessed after flying. That is, when there are data encryption and firmware failures at the same time,recovery costs and technical requirements will be quite high.

From the results, the newer the board number is, the greater the possibility of

data encryption is after swapping PCB. It is predicted that future laptop drives and mobile series will adopt this mechanism. Unlocking the firmware of new MRT update this time will definitely bring considerable convenience to the original board handling.

As for other situations that lead to the overcoming of the problem of data encryption, further research is needed to determine the scheme.

The above is WD 2.1.7.x content of the firmware unlocking tutorial. For more technical questions, please contact technical support:

William Skype: live:mrtpro_1  QQ 806944413

Wei QQ1368922240

Thank you for your attention and support. See you next time.