WD 2.1.7.x 固件解锁教程完整版

前言

相信 800xx 及以上系列硬盘一直以来给大家带来了相当大的困扰，比如购买解锁板需要额外支付成本，有些解锁板价格也相当高。另外，有些解锁板可能存在两个版本，有时读写 ROM 可能会引起电路故障导致损坏，从而进一步增加维修成本。

除了固件锁的存在给维修带来了麻烦，新系列硬盘还存在数据加密问题，即使用非原始板，数据存在加密情形。

MRT 最新版本 2.7.1.x 正式发布全新功能——WD 固件解锁，当前覆盖的 SATA 板号为 800065、800066、800077、810011，其最大优点在于使用原板即可解锁，无需转换板。

第一部分 WD 固件解锁准备工作

在 MRT 程序实现 WD 固件解锁需要三个条件：

①原始 PCB 板

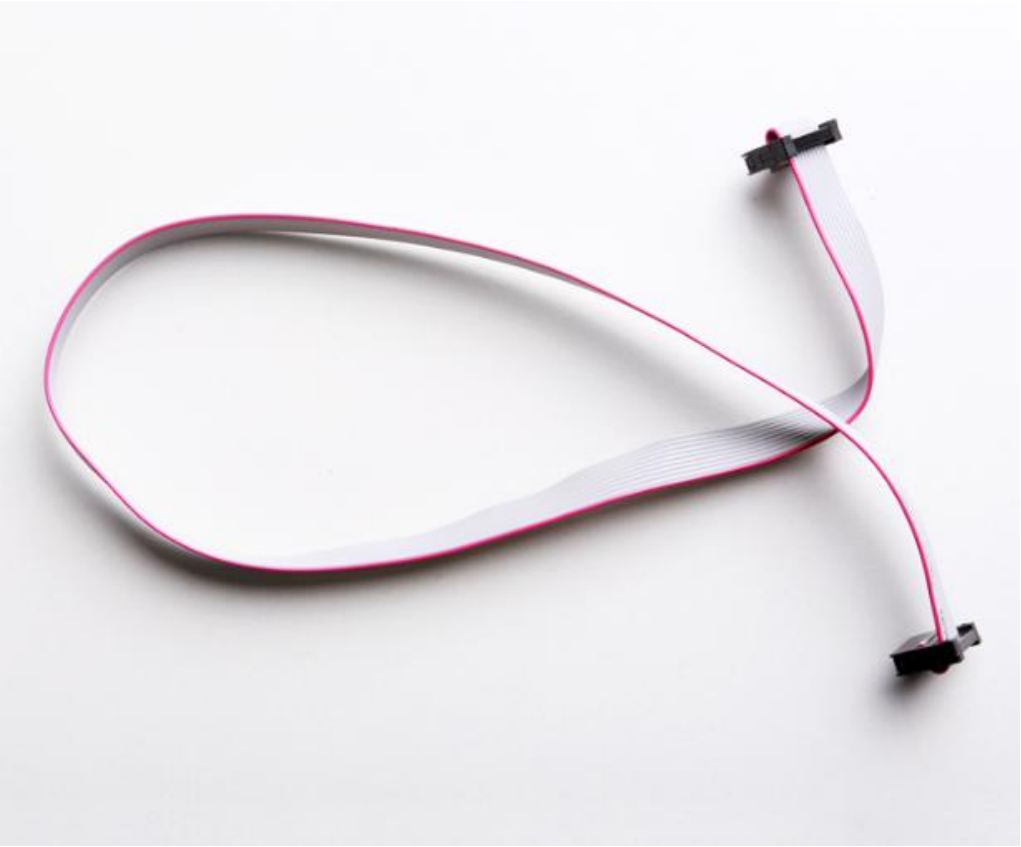
②编程器（推荐 MRT 编程器 3.0，速度、稳定性跟便捷性大幅提升）

③终端适配器（必须选择 WD 指令头）

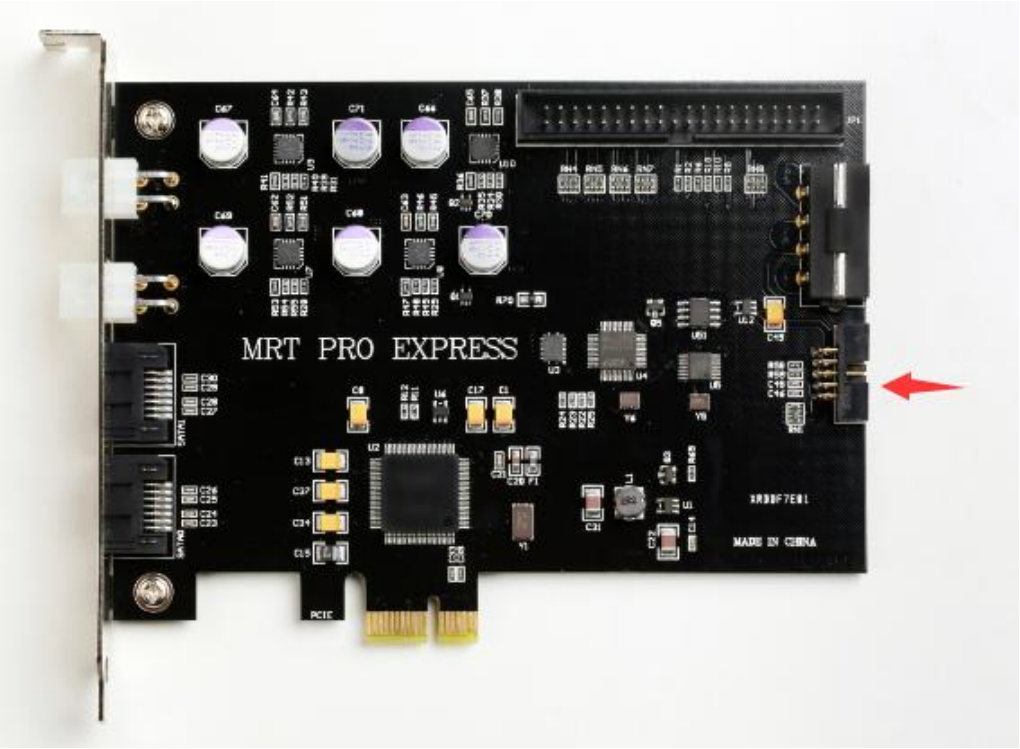
原始 PCB 板是应用固件解锁所必备的条件，相当多的新系列硬盘转板或换板将导致数据加密，为保证数据恢复，请使用原板进行解锁。

MRT 近期将发布一款全新编程器，即 MRT 编程器 3.0。该编程器的最大特点是增加了引脚，用以实现编程器与 ROM 的直连方式，同时针对 WD 的芯片做了深度适配，稳定性和兼容性更佳。因此，MRT 编程器 3.0 既可以通过解焊芯片的方式来实现 ROM 的读写，也可以通过引脚的方式从编程器直连到 ROM。

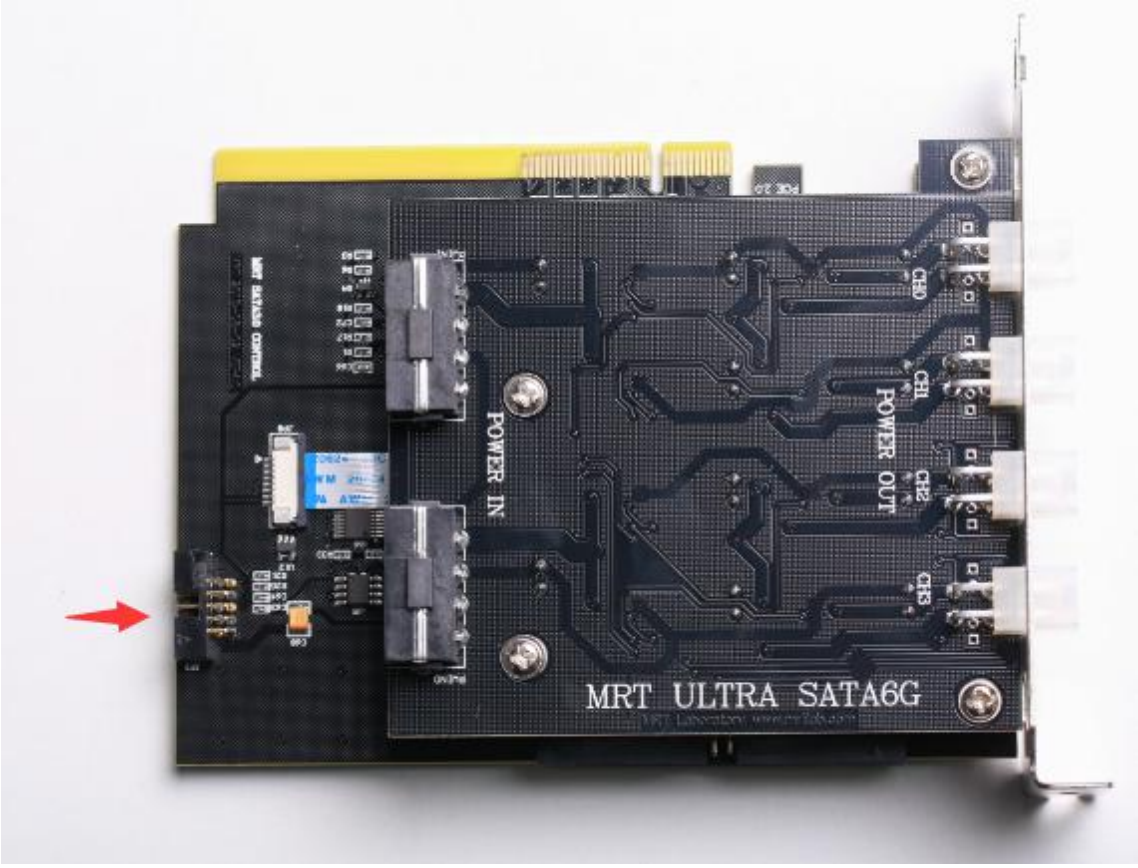
第二部分 编程器的连接



编程器线



MRT Express 编程器接口



MRT Ultra 编程器接口

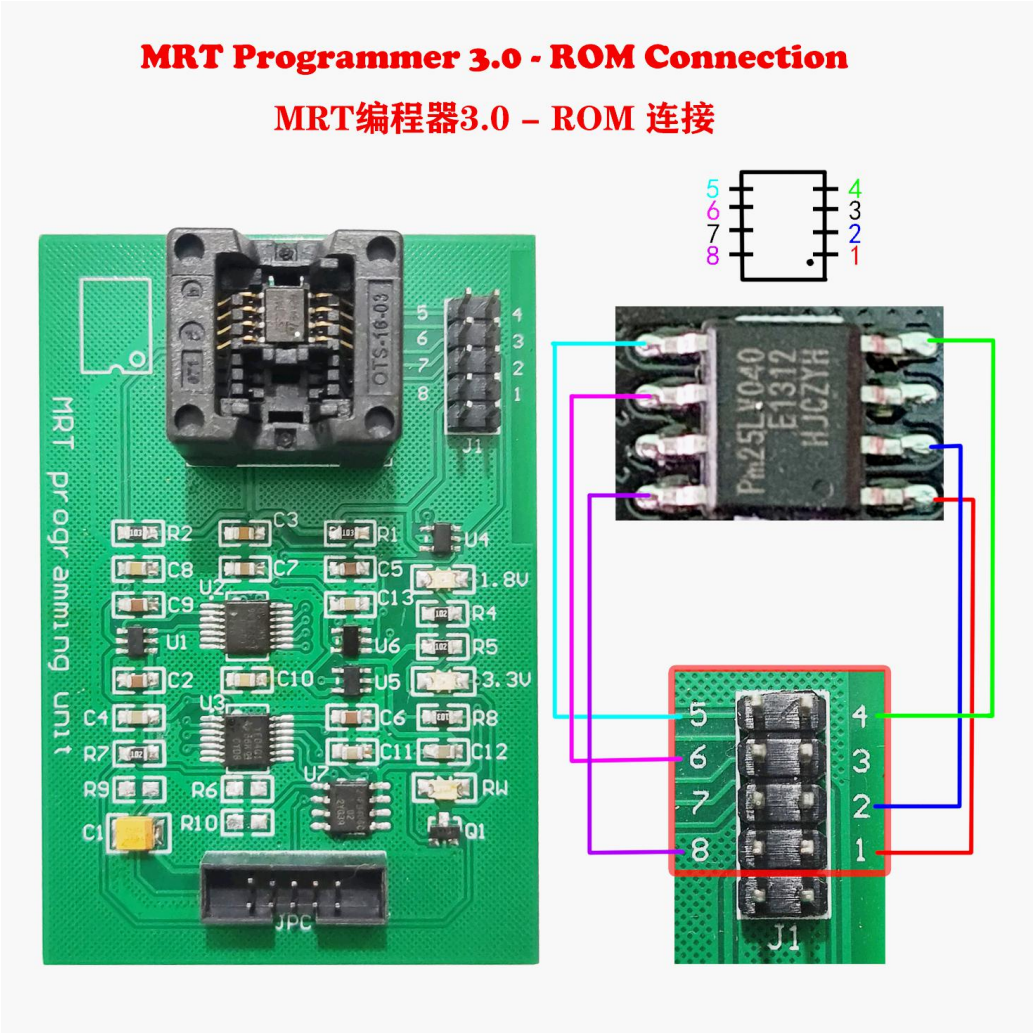
在连接编程器线到硬件卡的时候，请事先确认接口的方向。MRT 编程器线在设计的时候留有凸台，方便对准硬件卡的相应接口。

连接编程器线到硬件卡的时候，尽量扶住硬件卡的编程器接口，防止接口松动。有部分用户反馈当硬件卡在连接编程器线之后，报告“设备初始化失败”，一般都是端口松动或编程器线未连接好导致。

第三部分 编程器的使用

下图为西数 PCB 板的 ROM 芯片八脚编号与 MRT 编程器 3.0 的引脚编号，其编号是一致的。

注意：图片右上方有一个编程器示意图，右下角的黑点代表 ROM 芯片的小圆点，其图示方向即为左侧编程器的 ROM 芯片摆放方向，即小圆点应该朝向编程器中心。

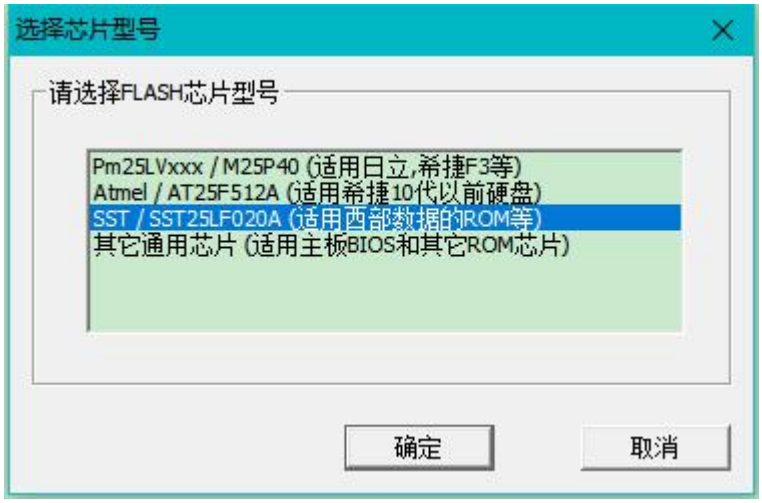


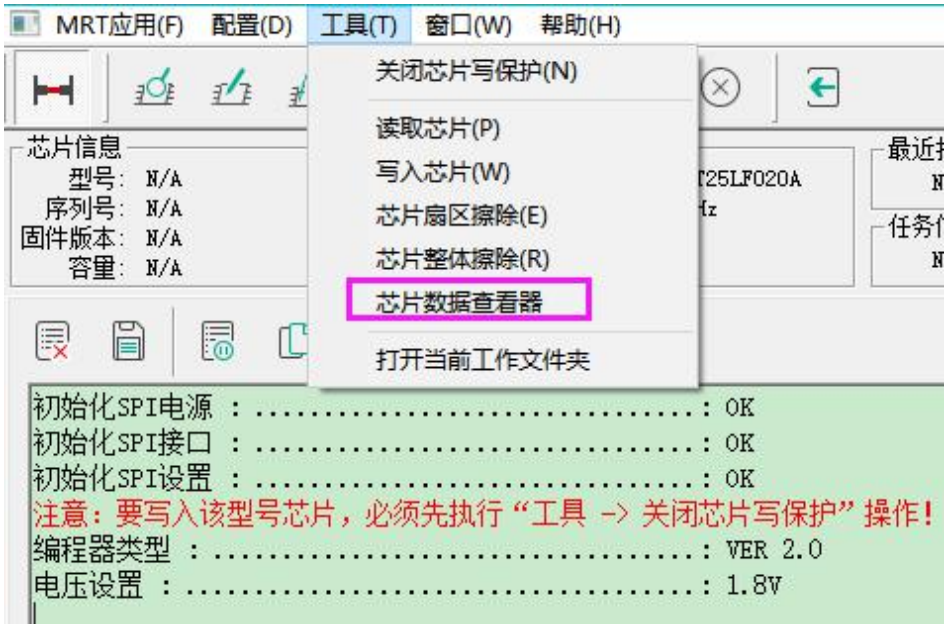
编程器与 ROM 引脚编号

使用 MRT 编程器 3.0 读写 ROM 有两种方法：

1. **常规法**：解焊 ROM 芯片，接入编程器，WD 程序在生成解锁 ROM 之后，将自动写入到芯片，再将 ROM 芯片焊回 PCB。该方法适用于所有盘，包括对 USB 盘读写 ROM 数据。

操作路径：主界面常规通用功能-ROM 编程器工具-选择适用 WD 的 ROM 一项-工具-芯片数据查看器，如图：


选择芯片型号
请选择FLASH芯片型号
Pm25LVxxx / M25P40 (适用日立,希捷F3等)
Atmel / AT25F512A (适用希捷10代以前硬盘)
SST / SST25LF020A (适用西部数据的ROM等)
其它通用芯片 (适用主板BIOS和其它ROM芯片)
确定
取消


MRT应用(F)
配置(D)
工具(T)
窗口(W)
帮助(H)
关闭芯片写保护(N)
读取芯片(P)
写入芯片(W)
芯片扇区擦除(E)
芯片整体擦除(R)
芯片数据查看器
打开当前工作文件夹
芯片信息
型号: N/A
序列号: N/A
固件版本: N/A
容量: N/A
初始化SPI电源 : ..... : OK
初始化SPI接口 : ..... : OK
初始化SPI设置 : ..... : OK
注意：要写入该型号芯片，必须先执行“工具 -> 关闭芯片写保护”操作！
编程器类型 : ..... : VER 2.0
电压设置 : ..... : 1.8V

芯片数据查看器
请输入起始字节地址:
0
请选择芯片容量大小:
32 KB
64 KB
128 KB
256 KB
512 KB
1024 KB
2048 KB
4096 KB
读取的字节长度:
1048576
确定
取消

常见 800xx 板号的 ROM 大小：

800022/41 - 512 KB

800065/67 - 1024KB

800066/69 - 1024KB

800077 - 1024KB

810011 - 1024KB

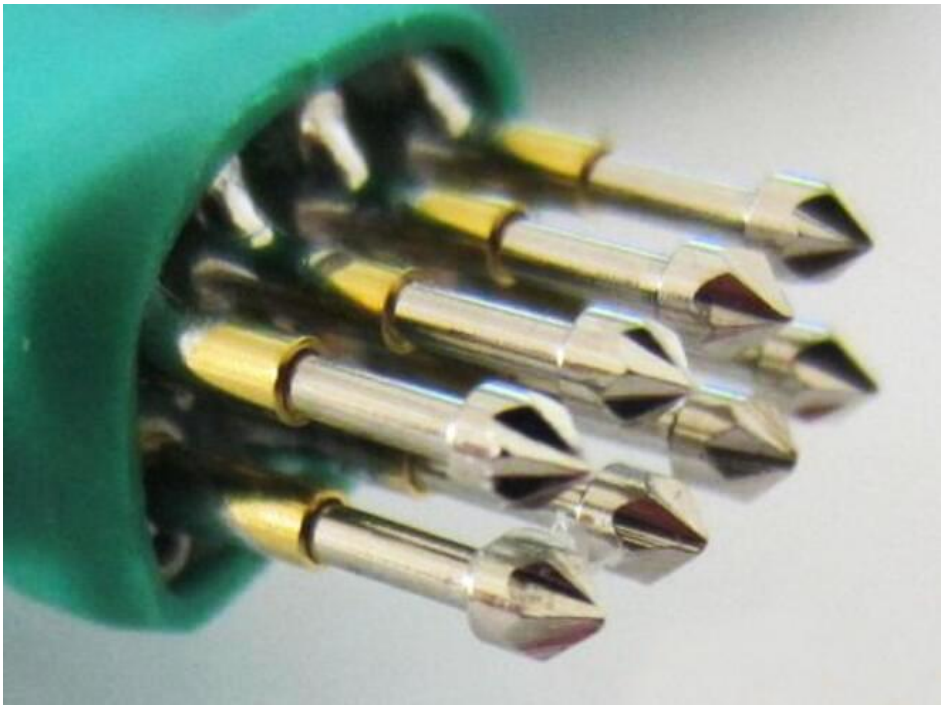
810035 - 512KB

选择好大小之后，备份好原始 ROM，之后就可以在 WD 程序中对其解锁。

2. **ROM 直连法**：通过引线连接编程器的引脚和 ROM 引脚，而 ROM 引脚存在 PCB 的正面引脚和背面引脚两种，即正面为 ROM 芯片的八脚，背面为对应的触点。

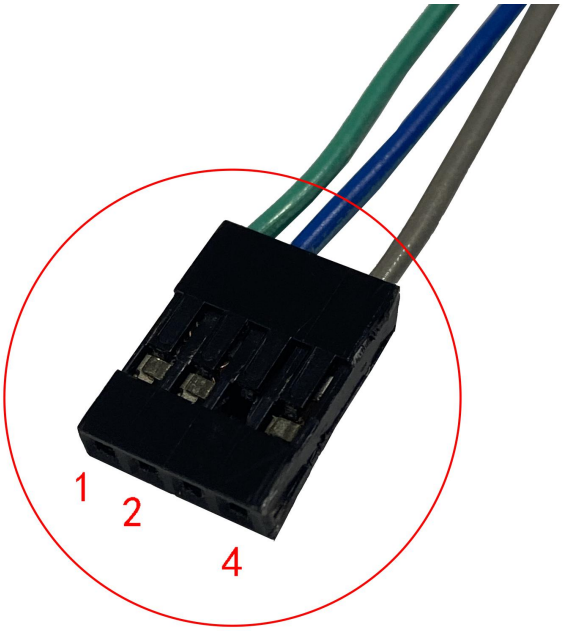
直连法需要认准编号，“编程器与 ROM 引脚编号”图示给出了 1-8 共八个编号，编号顺序为“U”型排列。在连接的时候，我们需要排除编号 3 和编号 7 的引脚。

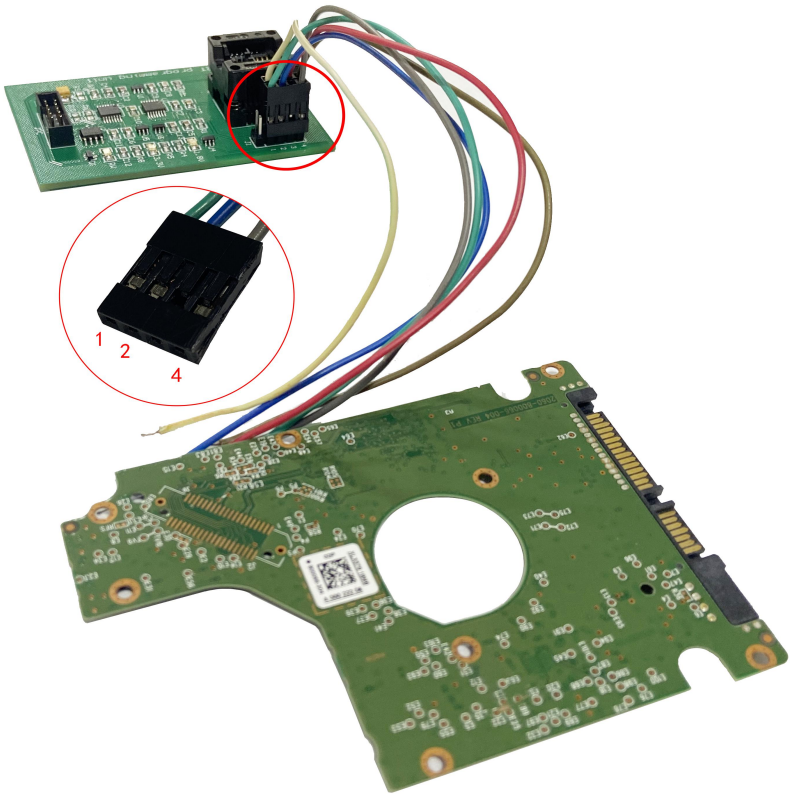
① 单接 PCB 的 ROM 直连法。“编程器与 ROM 引脚编号”图示的连线就适用此方法，此时需要拆下 PCB 板，借用**引线连接编程器到 ROM 的八脚**。如果有匹配的 ROM 烧录探针线，分别连接编程器引脚和 ROM 八脚，读写起来会更加方便，省去了焊接过程，如图：



② 不拆 PCB 的 ROM 直连法。该方法需找到 PCB 背面的相关 ROM 引脚点，再通过引线焊接的方式连接。当然，该方式相对麻烦了点，需焊接 6 个引脚点，有些引脚空位较小，对焊接技术有一定要求，后续我们会针对此方案进行研究，将来或许会有更好的方案进行替代。

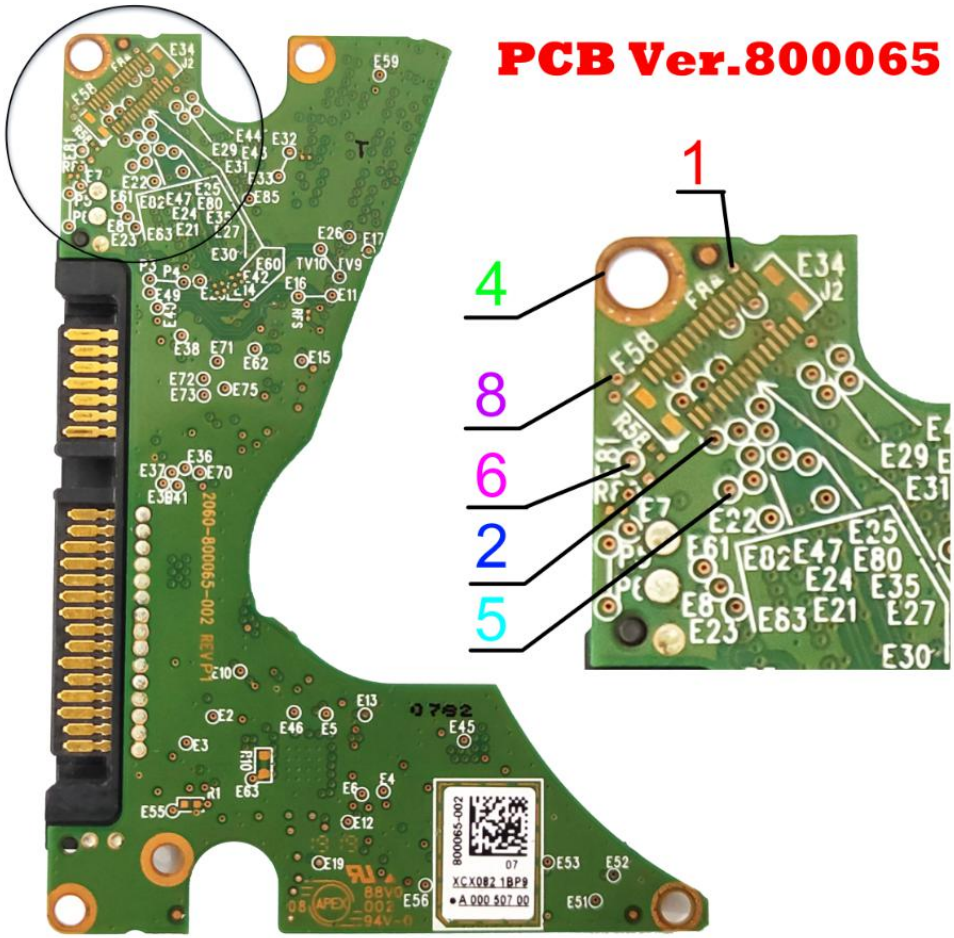
这里提供一个参考，比如 PC 主板跳线的连接线，如下图：

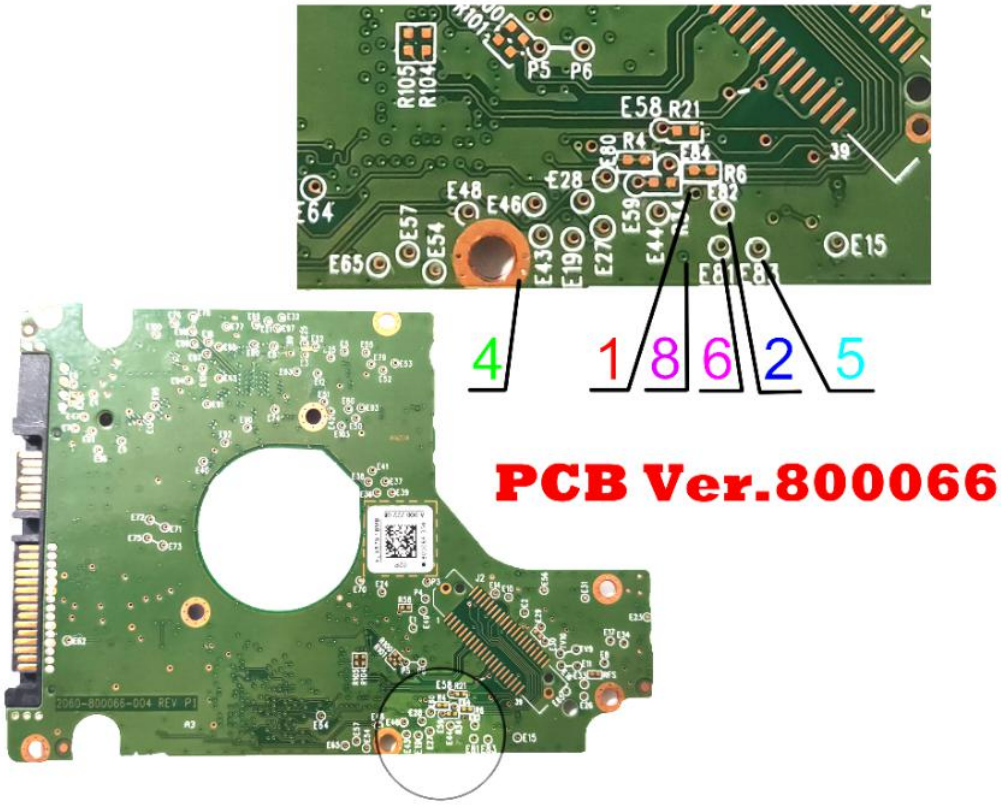


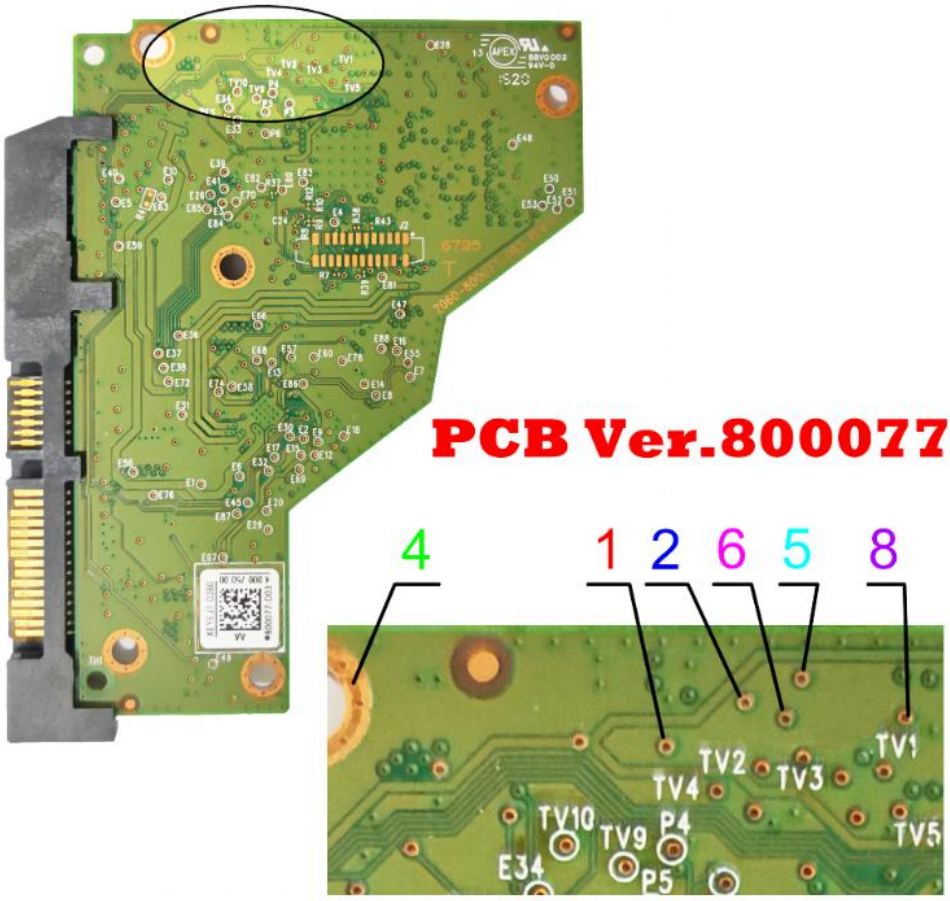


不拆 PCB 的 ROM 直连法示意图

如果采用该方式，需要对不同的 800xx 系列电路板板号进行比对，如下图：



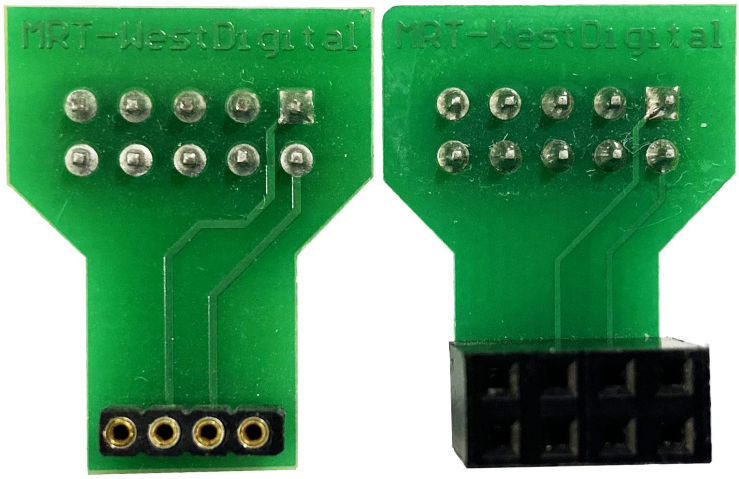

R105
R104
P5
P6
E58
R21
R4
E84
R6
E28
E48
E46
E64
E57
E54
E65
E43
E19
E27
E44
E81
E83
E15
4
1
8
6
2
5
PCB Ver.800066


PCB Ver.800077
4
1
2
6
5
8
TV1
TV2
TV3
TV4
TV5
TV10
TV9
P4
P5
E34

第四部分 终端的连接

请使用 MRT 的终端产品进行连接，指令头务必使用 WD 指令头。

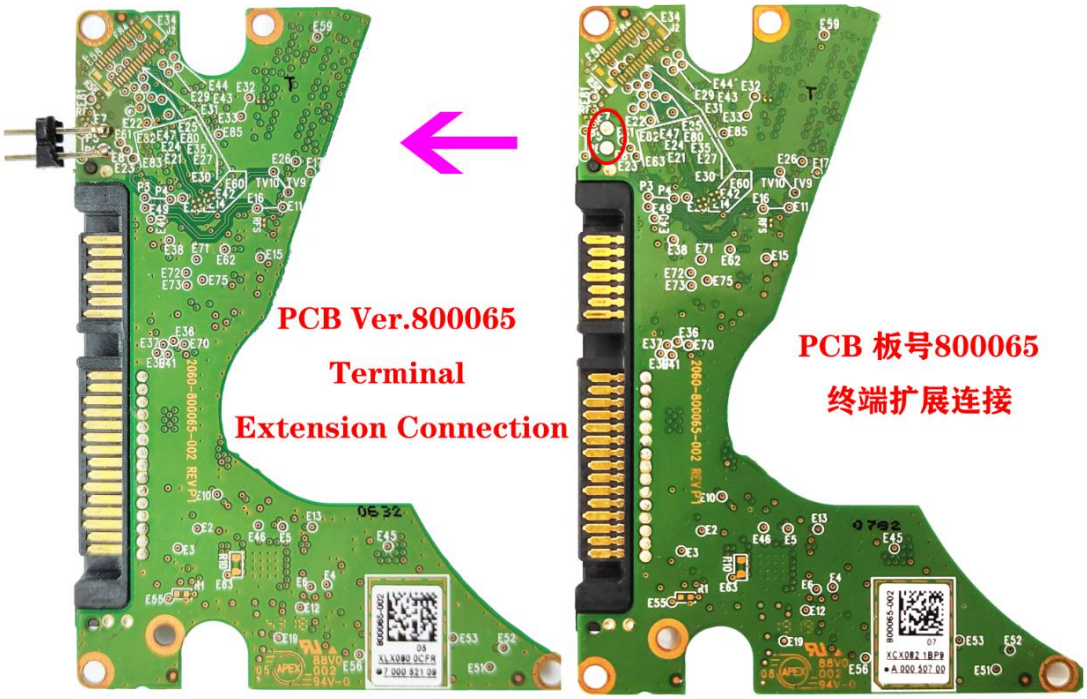
MRT 的指令头一共提供了八个，其中 WD 指令头有两个，一个适用于 2.5 寸硬盘，一个适用于 3.5 寸硬盘，见下图：

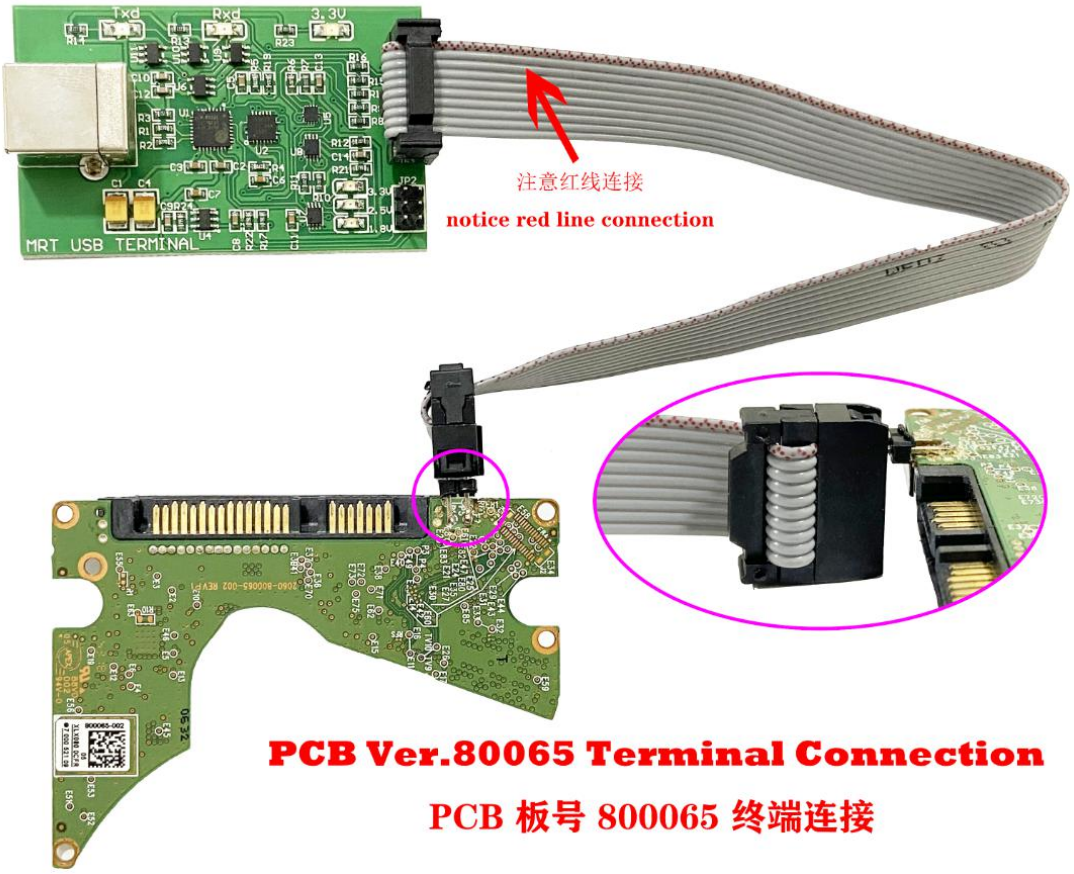


WD Connectors
WD 指令头

终端连接例外情形：800065 板号的串口接口十分狭小，无法正常连接，我们可以通过扩展触点的方式将其延伸，此时可以直接用 COM 口线进行连接，不需要 WD 指令头。

同样的情况，如果将来有新的板号存在类似的情况，我们可以参照下图进行连接：


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


Txd
Rxd
3.3V
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

软件界面的 COM 口选择：

在界面点击“终端连接”按钮，弹出的对话框可以选择 COM 口，如下图：

Prolific USB-to-Serial Com Port(COM 5)：新终端（PL2303）的串口 ID

Silicon Labs Dual CP2105 USB(COM38/39)：双核终端（CP210x）的串口 ID

第五部分 固件解锁

1.在家族面板手动选择家族。既然存在固件锁，家族无法获取，我们可以根据归纳的板号选择家族。由于同一个板号可以有多个家族，在不知道家族的情况下，可以手选任意一个进行测试。

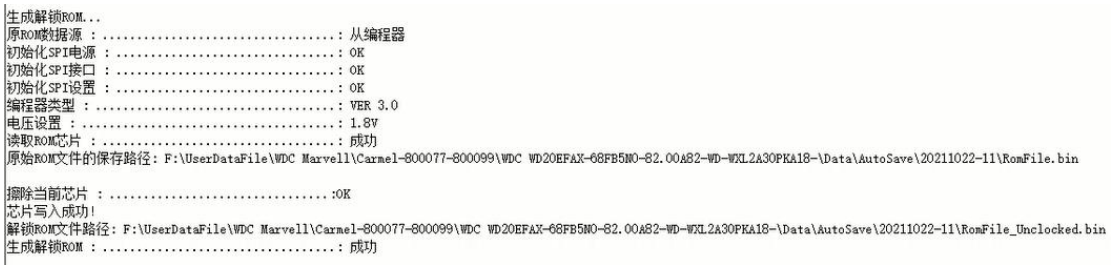
2. 路径：ROM 工具-生成解锁 ROM。

如果是提前保存的 ROM 文件，比如之前通过解锁板或解焊芯片备份下来的 ROM，我们选择“从文件”获取 ROM 来源，解锁后需在编程器应用程序手动写入解锁 ROM 至 ROM 芯片。

注意：请务必使用原始 ROM！

如果是采用直连 ROM 引脚或解焊 ROM 芯片的方式，我们选择“从 Mrt 编程器”获取 ROM 来源，在线读写 ROM，此时将自动写入解锁 ROM。

成功后如下图，软件将自动生成解锁 ROM 文件“RomFile_Unlocked.bin”：



3. 断电上电，硬盘在第一次握手前，在终端界面会显示“hello mrt！”的字样，此时说明解锁 ROM 已经生效，并请求握手完成最后的解锁步骤，我们可以点击右侧的“握手解锁”按钮:

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

4. 当我们保持程序的打开状态时，断电上电，软件将自动对硬盘握手解锁，无需再次握手。

```
握手解锁...
握手解锁 : ..................................: 成功
```

5. 当我们退出程序后，对硬盘上电，使用解锁 ROM 的西数硬盘会和希捷一样，出现长忙表现，此时我们需手动进入 WD 应用程序，在家族面板进行解锁握手，使其就绪，之后便可以正常访问固件了。

关于数据加密的说明：

从搜集的结果来看，WD 对于新一代 800xx 系列板号和固件做过多次调整，包含 SED 锁、固件锁、数据加密、板号的密集更迭等，其表现极为复杂：

USB 转 SATA，或带锁 SATA 转无锁 SATA，均存在有数据加密和无数据加密的情形。而早期有少量型号的 USB 盘转解锁 SATA 并没有这种情况，只需要遵循过去的数据解密过程即可。

关于加密成因，大家应该多少能猜到，主要算法在主控代码段，现有的分析手段非常有限，加密问题仅能通过飞线的方式处理。但飞线也有其局限，比如飞线后不能访问固件，即同时存在数据加密跟固件故障的时候，恢复成本和技术要求会相当高。

从结果来看，板号越新的盘，转板存在数据加密的可能性越大，预测将来的笔记

本和移动系列均会采用这一机制。那么，本次 MRT 的固件解锁对原板解锁必将带来相当大的便捷性。

至于其他情形导致数据加密这一难题的攻克，还需进一步研究以确定方案。

以上就是 WD 2.1.7.x 固件解锁教程完整版的内容，更多技术问题请联系技术支持 QQ 806944413 王、1368922240 魏，感谢大家的关注与支持。