本节内容实际上基本用不到 只适用于部分无法以正常方法搜索到作弊码地址的游戏

------------------------------------------------------------------------------------------------------------

源于 三国战纪2-群雄争霸 正值我改完三国战纪2-盖世英雄 欲于群雄上复刻一些功能时

发现此游戏的气值和无敌地址皆无法搜索到

偶然于论坛看到axdx前辈的自编译mamep0.168帖子里有提到这点 出自燕大侠之口

( <https://www.ppxclub.com/forum.php?mod=viewthread&tid=669494> )

其内容大致为若不修改可用地址检测 则无法搜索到d00000到dfffff区间的地址

而群雄的内存地址几乎都是800000-8fffff区间 但气值和无敌地址却在d00000之后

直接ci初始化有接近20w个地址被初始化



当输入cl并拉到最下方会发现其最大地址也只是b0ffff



既然如此 那就扩大搜索范围 从0开始到ffffff 理论上包含d00000-dfffff区间内地址



但不幸的是其最大地址仍为b0ffff

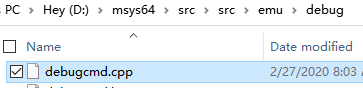


最后一个方法 直接初始化d00000-dfffff区间的地址

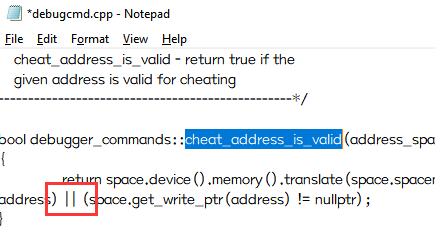


但是 没想到吧

于是乎 一番找关键词后定位到了



以文本编辑器打开 Ctrl+F搜索 cheat\_address\_is\_valid 并回车两次 会来到一个函数

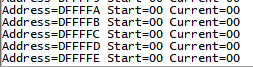


将红框处原来的 && 改为 || 即将与改成或 并重新编译

( 亦可注释此行 并在其下一行添加 return ture; )

重新编译后若直接ci初始化 最大地址依然是b0ffff

但若初始化d00000-dfffff区间 其最大地址就可以搜索到DFFFFE

------------------------------------------------------------------------------------------------------------

可能会有读者想问为何要将 && 改为 ||

理论上判断地址是否有效应有多个条件 此处 && 即当完全达成时才算有效地址

而 || 为达成其一时就算有效地址 故如此修改

------------------------------------------------------------------------------------------------------------

亦可能会有读者想问

为何本节内容不像上节一样搜索关键字 No writable bytes found in this area

然后将其相关语句注释掉 因为那一块是函数中的套娃函数 而非简单地两条调用输出命令

改了之后可能会影响其它地方的功能 不如按本节方法改表层函数的条件

可能会有更好更简单地方法

但实测按本节的方法修改后除了有用的无用的地址皆会初始化外 并无其它不良影响

其实际效果和axdx前辈修改的一致

------------------------------------------------------------------------------------------------------------

后来发现其关键字在帖子里燕大侠就发了 只是连着inline一起搜索不到 源码改过了