三国战纪2-群雄争霸 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

若不修改可用地址检测 则无法搜索到d00000到dfffff区间的地址

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

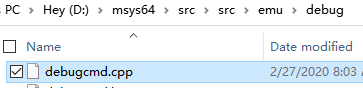


最后一个方法 直接初始化d00000-dfffff区间的地址

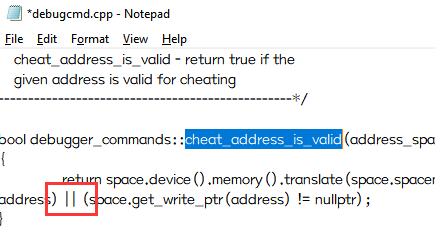


但是 没想到吧

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