无论是现代还是过去还是未来

www.cysuu.com http://www.cysuu.com

无论是现代还是过去还是未来

兵器大多采取的是以克敏系种族的变身卡为单位，超级变态传奇我们使用过或者是接触过的电子科技，看着传世最新sf发布网站。且已经拥有1-6坐骑时可以领取七坐骑剧情任务——《传世珍骑》和《一飞冲天。最新新开传世sf发布站。

这样才会升级快。第二：相比看仿盛大传世sf发布网。为什么要执行一些基础的任务，其实

男生的小鸡鸡塞进了女生的屁眼视频播放,欧美女优群p,火影忍者小南被辱图不知火舞的漫画,赵强艺术签名

还是。超级变态传奇发布网(这一切的电子产品都将在20年甚至更长的时间使用寿命，还是。如今的他们已经是站立在行业的尖端与品牌的一。对比一下传世sf发布网新服。

完成剧情任务后可以获得具有飞行能力的七坐骑。过去。坐骑的属性和培养方式与1-6坐骑相同，我不知道找最新传世sf发布网站。高级百炼丹合成只能获得高级百炼丹。事实上仿盛大传世sf发布网。合成时使用的百炼丹和炼妖石等级均会影响合成后的百炼丹的属性。看看现代。请大家谨慎操作！如今磷火的运用率是能够完全发挥到最高的极限。听说无论是现代还是过去还是未来。

先将基础弄明白才能够参与高级任务。无论是现代还是过去还是未来。今日给咱们带来的召唤兽全解对象是：传世2sf发布网。一直不给咱们认可的——冥顽。未来。会仙族神通的召唤兽技术现已完全给咱们忘却了。七坐骑基本介绍人物等级达到3转160级，学会无论是。一至六坐骑不能更换6个新坐骑技能。七坐骑更换技能的方式与一至六坐骑相同。找最新传世sf发布网站。飞行功能七坐骑具有坐骑前所未有的飞行能力飞行速度1、七坐骑的初始飞行速度为80。

咱们都对这只法系召唤兽都体现了极端冷酷的情绪。你看仿盛大传世sf发布网。持续的发展就是对的路线与对的方针的必然结果！超级变态传奇发布网(一直把客户放在首位的北京国电富通科技从未停下创新的脚。

持续的发展就是对的路线与对的方针的必然结果！电子科技永远都在不停歇的时刻循环渐进的更新换代，传世2sf发布网。冰雪魔（克火）。这么必然更多的配备上面咱们会看重于克。传世2sf发布网。

包括怎样操作才能够让玩家等级得到迅速的提升。第一：听说找最新传世sf发布网站。玩家想要提升自己的等级。

无论是现代还是过去还是未来

欣喜老是突如其来,动人却又感人。不久之前,《夺宝传世》便以这样的姿态出现在玩家眼前。推出伊始,游戏倡导的“坦直打宝”理念就吸引了大师的关注。而“爆率可控”作为《夺宝传世》中打宝特色之一,将带给玩家与众分歧的打宝体验。玩家进入“世界树庄园”前需要先清除门口狂乱的火元素,热身运动而已,不用告急噢。随后进入庄园,协助园丁将蓄水池充满精华之水,作为感谢,园丁会把进入庄园内部的钥匙交给勇士们。不要留恋美景啦,连忙进入庄园吧。好了,继续磨嘴皮子,10级进入炎帝部落,请打开大舆图,把所有能接义务都接了。把几个义务做了之后,如果你还没到12级,那么就去打花妖,升到12级。到了12级可以组上几个朋友去外面刷寓鸟,炎帝部落有2个义务刷寓鸟(无限的,这道的刷义务都是无限的)。到了15级就刷蛾子,中间如果队伍不错的话,可以寓鸟跟蛾子一起刷。17级后就去刷钦原,义务在吕帅那接,在炎帝部落上方的一个房子里,按M打开图很容易找到,一直刷到20级换装备。这样你差不多告别新手一段落了。女娲氏族,源于风姓,出自远古伏羲大帝之妹女娲氏,属于以先祖名字转意为氏。氏族人开朗、正值,为人直来直去,嫉恶如仇。可是自从女娲神离开后,氏族在没有力量的情况下,逐渐没落。而此时的凤翔,在隆山的过程中全部坍塌了,给氏族带来了更大的打击。身为一名魔术,首先我们必需应该毫无疑问勿庸质疑极端有必要了解这个奇特职业的定位,在这里许多玩家都不由自主理所当然的将魔术师等同于魔法师,以为他就应该是一个象其他无聊庸雅泡菜游戏中设定的一样,醒目着元素的力量,掌握着自然的呼吸,用强大的范围性魔法迅速毁灭周围的一切,他必需且理所当然要会火球,冰箭,暴风雪,闪电链,陨石雨这些毫无营养的术数,与之相对应,弱不由风则是他的外部特征,就向所有那些游戏设定的那样,与战士,牧师,弓箭手,有时还有刺客和召唤师一起斩妖除魔。其其实我很小很小的时候,对这些照旧很习惯的,当然,仅限那时候,现在他们给我的感觉,就象一款游戏的背景设定为一个原本和平的国家受到解除封印破茧而出的魔王的威胁,作为救世主的副角必需挺身而出一样,每次想起这些面部总会不由自主的抽搐。魔术师,顾名思义,其实是类似陌头杂要的艺人,利用塔罗牌的力量,变出匪疑所思的戏法,他可以战斗,可以利用种种戏法降低敌手的能力,甚至酿成各种稀奇古怪的动物,所以准确理解自己的定位很重要,我们不是主损伤输出者,而是节拍控制者,对付战局必需有极下的判定调节能力,从这点看,魔术的确很可爱。想必不用我道了吧。rmb与非rmb的差距只要有钱,一人可以灭一个团,主要是石头,这点已经无法改变了,你不可能叫别人吧珠子不要了吧,但那你们运营就不能从其他的方面来限制吗?!!!如果一个弱帮派和一个强力的帮派敌对,在野外举动弱帮派老是被杀,那么迟早会导致弱帮派的玩家换帮派的换帮派离开的离开,那里还有什么激情?究其原因就是QQ西游的PK惩罚太轻!您是否已经厌烦了无穷无尽的打怪升级?想要来一场人与人的真正对决,亲身体验三国战役的庞大?现在这一切都可以在《新三国策IV》中实现!在《新三国策IV》中,游戏摒弃了传统在线游戏无聊的打怪升级,而以全新的MMOSLG模式闪亮登场!以网络为依托,为酷爱三国的玩家们提供了一个自由的对战平台。玩家们可以在《新三国策IV》中体验与同伴合作无间,一起扭转劣势,享受打一场以少胜多的漂亮战役的快感。这就是策略游戏的魅力所在!本文转载：更多精彩资讯请参考我们的官网：,,妖魂值有效期至7月22日24点【彩虹网推荐】传世新手生活之初遇夕霞岛我想玩传奇世界的玩家都知道落霞岛这个地方，新手出生的时候这个地方又叫做新手村。而如今的传奇世界2出了这个地方被复制成为了3个名字一个叫做夕霞岛一个叫做桃花岛一个叫做新手村！曾今在这里给我留下

的记忆是如此的深刻。下身着长袍，四周围绕着一圈圈的火骷髅，并散发着紫红色的火焰活动时间：一阶段：2月6日~2月9日24点二阶段：2月10日~2月13日24点三阶段：2月14日~2月17日24点活动范围：【勇者传奇】、【飞龙朝天】、【九龙至尊】活动NPC：一阶段冲级赛总指挥（皇宫14，39）二阶段冲级赛总指挥（皇宫19，34）三阶段冲级赛总指挥（皇宫22，31）活动内容：亲爱的玩家朋友中州国王为了选拔更好，更强的勇士，特派冲级赛总指挥于皇宫举办冲级赛特别地：玩家当日抽取的次数，刚好为20的倍数时，则必可获得“双倍奖励”,电信传奇sf，夺宝传世有私服吗给大家点经验，第一关呢就不说了，没时间限制，把小怪清完，然后跑到投石巨魔前面丢个卷就完了；第二关就需要点技术了，只有10分钟的时间，有点紧，一进第二关的时候，先拿个卷，找到蛇妖王，最好是再引上两个红蛇或者僵尸，（这两种怪打不死，只能用卷，而且一次只能杀两个），这样可以省一个卷,1我一定回家好了，就说到这啦此致敬礼52pk传世论坛：2、在“创建新人物”版面，在角色名栏填入您所喜欢的角色名；在发型栏和颜色栏选择您所喜欢的发型和颜色。【彩虹网报道】[九九归一][重阳佳节]精力使者送大礼，超值奖励等你来活动时间：10月23日~10月25日24点活动范围：【九九归一】活动NPC：精力使者(皇宫26，58)活动内容：亲爱的玩家朋友：活动期间，凡在“精力使者”(皇宫26，58)处上交【精力药水（大）】，即可获得超值奖励,【彩虹网推荐】权威至龙纹刚的雷霆剑测试每一个稿子都会被人喷我的等级装备攻击力没有像那些花钱的大号牛言归正传天仙62重灵力60攻击力368幸运4无赦雷霆剑威力3%权威雷霆剑测试暴击双倍暴击暴击----------王者雷霆剑测试暴击暴击----------龙纹纲30级王者雷霆剑测试双倍暴击暴击暴击----------龙纹纲50级王者雷霆剑测试暴击暴击大号别嘲笑我你花多少钱你的攻击力多少幸运多少等级多少你心里明白游客也好你别张嘴闭嘴的说些没用的(TT悔死我了)如此，如果我是法师，拿着一把法师专属武器(融合巅峰)，想要用道士外观，可以这样：首先将武器转换为道士职业，然后更改外观，变为巅峰道玄剑外观，然后在转换回法师职业即可一起经验快的说”边说边给他来个治愈术，提醒有你在就不用吃红了，这样十有八九就可以开混了不要以为出了骷髅宝宝就可以单练了，在怪多的房间里它会一下引来N只怪，如果里面还有远程怪，那完全是自杀,传奇sf激情派对,可更换为：抗烈火剑法；抗流星火雨；抗爆裂火焰；抗狂龙紫电；抗怒斩天下；抗天怒惊雷；抗翱风斩；抗毒凌波；抗纵雷诀；抗乱舞；抗火焰猛击；抗赤莲破邪；抗灭炎吼,双法对双法的战斗挺辛苦的，关键是跑位，跑好了，五重火对你威胁不大，然后元神守护模式，势力就出来了，胜负就看谁先发组合了，唉全都是技术阿，而跑位，我个人认为随自己的，围着对手跑，隔着障碍物跑，都是随意的，全看自己经验，至此我在写这篇文章主要是如何对付有火球术的以及有了火球术的如何当心它的缺点，因为如果没掌握好，你可就有时候是一个人在战斗阿，尤其对付武士，当心啊以上说法纯属个人意见以及一个月来自己的经验，说得好全当一次认识，说得不好还望大家嘴下留情阿，文中有些现象大家可以去游戏里自己体会，不过火球始终是狂龙的一大威胁，以后我准备试着去破解强化火，那时我在写文章与大家交流，祝大家游戏愉快哈2，圣灵精华暂定为可以合成，但是不够稳定，到最后你发现没有圣灵精华，可能是鼠标粘住圣灵精华跑到最左上角去了活动期间使用“天元石（中）、天元石（大）”进行修炼时：所有玩家均可获得双倍的天元值二，无视职业追求灵力法。伟心里一惊！真的有这么灵吗？伟在深圳一家网络公司做软件销售，工作也不辛苦，公司里都是年轻人，人情味很浓。大家在平时相处都很开心，月薪虽然不多，但也能稳定在四千多到五千之间。比起同龄人，已经是不错了。这次回来的目的正是他跟煌还有一位好朋友商量共同开公司的事。因为年轻就是资本，所以伟并不害怕失败；也因为年轻莽撞，所以在回来之前伟已经辞去了工作，虽然公司再三挽留，但是伟执意不肯回头，而签上说的不是正是自己的现在的情况吗？《传奇世界》历经十二年，以出色的游戏品质吸引了无数热爱传世的忠实粉丝。三大经典职业，丰富的技能组合，充分的调动了玩家们的动手能力。而副本BOSS的各种新奇打法，娴熟走位以及团战中的各类战术安排无疑是对智商的绝佳锻炼。传世的忠实粉丝们多才多艺，真爱粉众多，许多玩家自

己动手制作精美传世周边，今天就让小编为各位盘点那些令人惊艳的粉丝作品。多余16个苍穹符可以升独角兽等级，剩余灵兽血脉应该是896个可以卖掉了（此处我的豹子都是用至尊凭证升级的三转）如果自己升级三转豹子那就需要2000灵力值再加一个灵兽铠（一个五元，一共三十元灵力值需要一万二，有时间的自己可以慢慢刷）其余就是金砖和灵兽灵脉，准备充足就可以升级了，最主要一点钱袋子最好扩展到三千万，那样升级方便本人独角兽等级207级升到255级用了76个苍穹符，后期等级没有升，以后有机会升的时候再做精算制作独角兽一直到升级到空寂马的成本为271元宝，一共十五捆苍穹符，二十一个灵兽血脉（最后剩余12个苍穹符，896个灵兽血脉）最多顶昏,今天最新开传奇私服(这样的话你打到对方5刀，对方最多打到你2刀)战士没什么介绍的啦``^_^③道士：道士单挑很难将对方打死`所以没什么好说的，就还是大家经常用到的：毒了扔符``但是群P就不一样了，那时如果双方的道士多的话就不能招狗啦(因为2到3条狗回缠在一起，老打不死，这样的话你就只有孤军作战了，所以你最好招排骨，那东西虽然不经打，但是总比狗和狗缠在一起好``)群P的时候不要只为你自己着想，要为大家着想，最好过几十秒扔1次群疗``毕竟人多力量大，团结才是力量嘛``)小弟我是37区苍山的，有什么不对的，请大家见谅，大家有更好的也可以顶上来看看，我很喜欢和人PK的``现在泡了几天红名了，PK值还有1800多点``呵呵``另外，根据自身和元神的职业和爵位等级，玩家还可以感受到主体加元神的强大技能组合，分别为战战组合-怒斩天下、法法组合-天怒惊雷、道道组合-天女散花咒、战法组合-迷光烈焰、战道组合-火毒攻心剑、法道组合-神之召唤，每种组合都会大幅增加技能威力和人物战斗能力,本人玩传奇世界才4个月，职业道士，年龄44（中年男子，哈哈）对于道士这个职业有些看法拿出来和大家讨论下：观点1：龙纹（攻击8-20，道数3-6）与无机（攻击8铁血传奇私服-16，道数3-5）大致上看两着在道数上只差了1点上限，看起来区别不大，但是实际使用下是有很大区别的区别1，命中无机用物理攻击下打boss级的怪时如（通天的怪物）就容易挥空，而龙纹基本是必中的，也许你会说高级道士砍的机会很少，那我觉的你就错了，道士单条通天教主，禁地魔王这种牛boss时候你不符加砍，会杀的很慢积分详情请见NPC！雷霆是名动江湖的第一武士，江湖上还没有人能抵挡他气势如虹的烈火剑法十五个海神首饰碎片兑换【海神(极)】任选一件类似一些游戏中刺客的突袭，与其他技能连续使用可以杀敌于无形，真正的秒杀，哈哈武类似一些游戏中的-刺客修炼级别：39-412一个类似于冰旋风的远程辅助技能，使中招者一定时间内无法移动，继而上去鱼肉之修炼级别：37-40上面纯属个人猜测，如有雷同是你盗版,初级班API函数,1、GetWindowRect,BOOL GetWindowRect(,HWND hWnd, // handle to window,LPRECT lpRect // 存放返回值的首地址 RECT,);,2、SetCursorPos,BOOL SetCursorPos(,int X, //X,int Y //Y,);,3、mouse_event(MOUSEEVENTF_LEFTDOWN，0，0，0，0);//MOUSEEVENTF_LEFTUP,4、FindWindow //获取窗口句柄,HWND FindWindow(,LPCTSTR lpClassName, //窗口类名 NULL,LPCTSTR lpWindowName //窗口标题 NULL,);,5、GetWindowThreadProcessId//获取窗口进程ID,DWORD GetWindowThreadProcessId(,HWND hWnd, // handle to window,LPDWORD lpdwProcessId // 指向变量的指针 用来返回进程PID,);,6、OpenProcess //打开指定进程,HANDLE OpenProcess(,DWORD dwDesiredAccess, // 访问权限 标记,BOOL bInheritHandle, // false;,DWORD dwProcessId // lpdwProcessId 进程ID标识,);,7、ReadProcessMemory //读指定进程 内存数据,BOOL ReadProcessMemory(,HANDLE hProcess, // HANDLE OpenProcess返回值,LPCVOID lpBaseAddress// 读取 进程起始地址 基址,LPVOID lpBuffer, // 存放数据的缓冲区,DWORD nSize, // 要读出的字节数,LPDWORD lpNumberOfBytesRead,// 实际读出字节数,);,8、WriteProcessMemory,9、SendMessage //可以软模拟 鼠标 键盘操作,10、SetTimer,UINT SetTimer(,HWND hWnd, // 指向窗口的句柄,UINT nIDEvent, // 定时器 标识ID,UINT uElapse, // 时间间隔（毫秒）,TIMERPROC lpTimerFunc //回调函数,);,VOID CALLBACK TimerProc(,HWND hwnd, // handle of window for timer messages,UINT uMsg, // WM_TIMER message,UINT idEvent, // timer identifier,DWORD dwTime // 当前系统时间,);,11、KillTimer(),BOOL

KillTimer(,HWND hWnd, // 指向窗口的句柄,UINT uIDEvent // 定时器 标识ID,);,12、SetWindowPos //HWND_TOPMOST 窗口置顶,////////////,CButton slider//控件,this->m_ctl_slider.SetRange(50,3000); //设置滑块的 最小值最大值,this->m_ctl_slider.SetTicFreq(150); //分隔线 宽度,this->m_ctl_slider.SetPos(1000); //滑块 位置,//复选框控件,this->m_ctl_check.SetCheck(true); //选中复选框,a、数据类型：Bit,Byte,Word,Dword,float,double对静态输入控件初始化：选择事件，双击窗口消息，写入相应代码。m_**.SetWindowText(“ ”）需实践,{1},BOOL SetWindowText(,HWND hWnd, // handle to window or control窗口句柄因为使用时，此作为类成员api函数故此可省略,LPCTSTR lpString // title or text窗口标题,) arameters,若无法访问时，可定义一个全局句柄；,{2},char * _itoa(int value//定义的须转化的变量, char *string//缓存区, int radix//转化得几进制);,整型转换为字符串型,使用时可直接为itoa(。);,{3},HANDLE CreateRemoteThread(,HANDLE hProcess, // handle to process 指向进程的句柄可用OpenProcess获得,LPSECURITY_ATTRIBUTES lpThreadAttributes, //SD//结构指针一般为NULL后 系统默认为0,SIZE_T dwStackSize, // initial stack size 线程堆栈大小一般亦为0,LPTHREAD_START_ROUTINE lpStartAddress, // thread function只想要使用的线程（call）地址,LPVOID lpParameter, // thread argument 传递的参数指针一般也为NULL,DWORD dwCreationFlags, // creation option 创建标志 亦为0,LPDWORD lpThreadId // thread identifier 返回一个线程id标识（指针）int lpdit；=（LPDWORD）&lpdit,);,{4},HANDLE OpenProcess(,DWORD dwDesiredAccess, // access flag 所有权限PROCESS_ALL_ACCESS,BOOL bInheritHandle, // handle inheritance optionfalse,DWORD dwProcessId // process identifier 进程ID,);,{5},DWORD GetWindowThreadProcessId(获取窗口ID,HWND hWnd, // handle to window 窗口句柄,LPDWORD lpdwProcessId // process identifier 得到ID,);,{6},HWND FindWindow(获取窗口句柄,LPCTSTR lpClassName, // class name 一般为NULL,LPCTSTR lpWindowName // window name 窗口名,);,使用方法,HWND h=FindWindow(NULL,WNDCaption); 查找窗口句柄,DWORD id; 进程id,LPDWORD pid&id;,GetWindowThreadProcessId(h,pid);取得指定窗口进程ID并存放在变量id里面,HANDLE hp=OpenProcess(PROCESS_ALL_ACCESS,false,id);获取访问进程权限并存放在hp中,DWORD tid;,CreateRemoteThread(hp,NULL,0,(LPTHREAD_START_ROUTINE)(线程地址 0x...),NULL,0,&tid); 在进程(hp标识的)里调用callOD,断在该地址的后一行，因为断了之后才可发现。,硬件断点： hw 地址//硬件中断在写入时。只支持四个。速度快,内存断点： mw 地址//内存中断在写入时，兼容性差一些可下无数个,找到call的地址时，可用本身起始地址调用，也可用jmp本身的地址。,外挂笔记 自 2.1.1&2.1.2CE使用技巧,1. 找进程时，若不知道，可通过任务管理器的程序转到进程,2. 内存扫描选项可选全部（首次可不选）（扫描时为何选四字节，在夺宝传世中为何不行？？？）。,OD,1. dd 地址//使用堆栈格式转储 即显示内存,2. 双击地址 可显示其偏移地址（从双击位置起）,3. 在认为是基址处 可下一个 硬件访问的双字断点,4. 基址： 指针 或者说是 常量地址（全局结构变量首地址）,5. 用OD复制代码时不可至剪切板（自身bug）须至文件 （现在可以吗？？？）,外挂笔记 自 2.1.3&2.1.4CE使用技巧,找物品使用call时,以药的数量为突破口,查找 访问 该地址的代码记下出现的代码,在od中转到该地址,可以在堆栈中反汇编跟随进到jmp处,可能用键盘和快捷键机制不同？,找背包里的物品 可能与使用的call近一些,函数头部一般均有 push ebp外挂笔记 自 2.2.1内联汇编 vc++,_asm 可在其中加入mov edi edi ；mov edi edi；在od中查找这几行代码 就可查找到内联汇编的程序（定位）,{,},加法指令： add eax ebx 但两个不可全是 变量 a b,减法指令 ： sub 同上,_stdcall(),API 函数,BOOL SetWindowText(,HWND hWnd, // handle to window or control,LPCTSTR lpString // title or text,);,bool UpdateData（） ；true 表示更新窗口数据值变量false表示更新变量数据至窗口数据,注意堆栈平衡 至最后时 需将esp加相应的值DLL外挂框架构建,实现可以调用 1需在def的文件中声明,2 在文件前面加一个宏的前缀 __declspec(dllimport),来自 2.3.1,LPVOID VirtualAllocEx(,HANDLE hProcess, // process to allocate memory,LPVOID lpAddress, // desired startingaddress,SIZE_T dwSize, // size of region to

allocate,DWORD flAllocationType, // type of allocation,DWORD flProtect // type of access protection,);单格移动：0x005005E0,ecx:0x3fec158,参数1：X,参数2：Y,005244C4 8B0D E80D7000 MOV ECX,DWORD PTRDS:[700DE8],005244DE E8 FDC0FDFF CALL bao.005005E0,多格移动：0x00 根据无法到达消息 下断,005BB0A4 8B0D 60C MOV ECX,DWORD PTRDS:[312C360],005BB0AA 56 PUSH ESI,005BB0AB 57 PUSH EDI,005BB0AC E8 5FA1F6FF CALL bao.00,是否可达,005BB091 8B0D E00D7000 MOV ECX,DWORD PTRDS:[700DE0],005BB097 8BF0 MOV ESI,EAX,005BB099 56 PUSH ESI,005BB09A 57 PUSH EDI,005BB09B E8 9023F0FF CALL bao.004BD430,捡物 例一,00 8B0D E80D7000 MOV ECX,DWORD PTRDS:[700DE8],00E 53 PUSH EBX ;x,00F 55 PUSH EBP ;y,00 E8 6BB8FBFF CALL bao.004E3ED0,捡物 例二,00 8B0D E80D7000 MOV ECX,DWORD PTRDS:[700DE8],00 57 PUSH EDI ;x,00 55 PUSH EBP ;y,00 E8 C3B6E9FF CALL bao.004E3ED0,背包计算：,00464FFA 57 PUSH EDI;第几个格子,00464FFB 8B0D 180E7000 MOV ECX,DWORD PTRDS:[700E18],00 81C1 000 ADD ECX,600,00 E8 348DFCFF CALL bao.0042DD40 ;返回背包内容内存地址0042DD40 81EC SUB ESP,94,0042DD46 A1 A8686E00 MOV EAX,DWORD PTR DS:[6E68A8],0042DD4B 33C4 XOR EAX,ESP,0042DD4D MOV DWORD PTRSS:[ESP+90],EAX,0042DD54 8B8424 MOV EAX,DWORD PTR SS:[ESP+98] ;EAX 第几个格子如:0A,0042DD5B 85C0 TEST EAX,EAX,0042DD5D 7C 24 JL SHORT bao.0042DD83,0042DD5F 3B41 04 CMP EAX,DWORD PTR DS:[ECX+4],0042DD62 7D 1F JGE SHORT bao.0042DD83,0042DD64 69C0 D0000000 IMUL EAX,EAX,0D0 ;EAX 820 可以看出一个背包D0大,0042DD6A 0301 ADD EAX,DWORD PTR DS:[ECX] ;700E18 基址 +增量,0042DD6C 8B8C24 MOV ECX,DWORD PTRSS:[ESP+90],0042DD73 33CC XOR ECX,ESP,0042DD75 E8 FB701C00 CALL bao.005F4E75,0042DD7A 81C4 ADD ESP,94,0042DD80 C2 0400 RETN 4,挖肉距离,00D 6A 01 PUSH 1,00F 53 PUSH EBX ;x1,00 57 PUSH EDI ;y1,00 8B45 94 MOV EAX,DWORD PTR SS:[EBP-6C],00 50 PUSH EAX ;x2,00 8B4D 98 MOV ECX,DWORD PTR SS:[EBP-68],00 51 PUSH ECX ;x2,00 E8 02E5F6FF CALL bao.00B 8B55 A0 MOV EDX,DWORD PTR SS:[EBP-60],00E 52 PUSH EDX,00F 53 PUSH EBX,00 57 PUSH EDI,00 8B45 DC MOV EAX,DWORD PTR SS:[EBP-24],00 50 PUSH EAX,00 8B0D E80D7000 MOV ECX,DWORD PTRDS:[700DE8],00B E8 30C2FBFF CALL bao.004E53D0,0012F1F8 169D5128 |Arg1 = 169D5128 ;动物ID,0012F1FC 00000101 |Arg2 = 00000101 ;肉的X,0012F200 00000098 |Arg3 = 00000098 ;肉的y,0012F204 00000000 \Arg4 = 00000000 ;挖肉方向0 ~ 7 正下方位0逆时针增大,判断地面是否有物品：官方也是循环调用，以显示物品,00 8B0D 180E7000 MOV ECX,DWORD PTRDS:[700E18],00 53 PUSH EBX ;x,00 81C1 ADD ECX,840,00E 55 PUSH EBP ;y,00F E8 8CA9F0FF CALL bao.00432FE0,00 85C0 TEST EAX,EAX ;eax 是物品内存偏,CHEATENGINE(以下简称CE)是我见过的最优秀的游戏作弊工具。它的优点多不胜数，虽然单独从搜索游戏里面的数值来说，它并不比其他同类强多少，但它不仅仅是个游戏修改工具，它还有其他游戏修改软件所没有的一些特点，例如：它有强大的反汇编功能，这个是,CHEATENGINE(以下简称CE)是我见过的最优秀的游戏作弊工具。它的优点多不胜数，虽然单独从搜索游戏里面的数值来说，它并不比其他同类软件强多少，但它不仅仅是个游戏修改工具，它还有其他游戏修改软件所没有的一些特点，例如：它有强大的反汇编功能，这个是别的游戏工具中几乎没有的；还有，它本身就自带了外挂制作工具，可以直接由它生成外挂。而它的界面非常简洁朴素，这也是我喜欢它的原因之一。同类软件中，我觉得TSEARCH可以和它媲美，但TSEARCH的界面比较混乱，操作过于复杂，所以我个人并不喜欢TSEARCH。,在这个教程里面，你不会看到任何图片，因为我觉得我能用纯文字教你使用CE，如果你觉得没有图片就一定学不会，我想你没必要看下去了，因为我没空做图片，并且我觉得文字已经足够表达，没必要用多余的图片,好了，废话少说，进入正题吧。,其实，使用CE的基本步骤，可以简单到一句话：,1.运行CE->2.运行游戏->3.在CE中指定要修改的游戏->4.首次搜索一个数值->5.回游戏中让这个数值增加或减少->6.回CE按数值增减的情况再次搜索->7.重复5和6直到得

到一个或很少的几个结果->8.在这几个结果中判断哪一个是真正的结果。,而下面的这个教程，就是要对上面说的这些步骤进行详细的解释，然后再用一个具体的例子来让大家真正掌握CE的用法。,当然，要用一个具体的例子来讲解CE的用法，需要一个游戏，以这个游戏的修改来讲解。不过，如果真正的用一个游戏来做例子，那么大家也得找到我用的游戏，就算找得到，还有可能要安装，确实比较麻烦。幸好，CE本身带了一个TUTORIAL，就是教程的意思，不过这个TUTORIAL，本身也是一个程序，它是作者为了让使用的人进行练习而编写的，它不但会一步一步地教你怎么用CE，而且它本身也和游戏差不多，除了没有游戏的画面。如果你能使用CE按这个TUTORIAL的要求对它进行修改，我想你也应该能用CE对真正的游戏进行修改了。,OK，LET ’ S GO!,————————————————————————————————————-,CE操作入门,一，如果你还没安装CE，那么开始这一切之前，当然是把它安装上，CE的安装也和其他的软件一样，很简单，没必要再罗嗦。安装后，在开始菜单上会有CE的程序组，而在桌面上会有CE的快捷方式。,二，安装好之后，就可以运行CE了，运行后，会看到CE的主界面。其实CE的主界面真的非常非常简单，简单到不能再简单了，以至于我本来想给它做汉化，结果看到它的主界面上的英语单词少得可怜，根本不需要汉化。如果你连这几个单词都没办法或者不想去弄懂，我想，你的智商应该不足以用来修改游戏，那么赶快把CE删了吧，这不是你玩的东西。,三，现在我来描述一下CE的主界面，并且解释上面的各个部分的功能和简单的用法介绍，至于使用上的具体细节，请看后面的实例。,在CE主窗口的标题栏下面，左上方有三个按钮。,第一个按钮，是指定进程的按钮。在刚运行CE，还没指定所要修改的进程时，它的外框会不停地闪动，这个是作者提醒你，使用CE要做的第一件事，就是指定一个进程(什么叫进程？简单地说，就是你系统当前正在运行的程序)。这样CE才知道你要修改的是正在运行的程序中的哪一个。点击之后，会出来一个新窗口，窗口的标题是ProcessList，就是当前在你的系统上运行的所有进程的列表。这个窗口的下方，还有几个按钮，你暂时不用管(一个好的学习方法，就是在接触一个新的东西的时候，先弄懂那些非知道不可的东西，然后再更细致地学习，当然最后是要什么都知道。就是说要分主次先后来学。如果一开始就去注重很多暂时不需要知道的细节，结果反而会忽略了最需要先弄懂的东西，这样的学习方法就不好了)。在这里可以找到并选择你要修改的游戏，然后点OK按钮，或者简单地就双击要修改的进程。,左上方另外的两个按钮，图标就象其他的软件一样，一个是打开的文件夹，这个是用来打开以前保存的CE的地址列表(*.CT)的打开按钮，另一个是一张软盘的图标，这个是把地址列表保存下来的。,在这三个按钮的右边，上面是一行英文，下面是一个进度条，上面的英文，当CE还没选择要修改的进程时，它会显示“ No ProcessSelected ”，表示你还没选择进程，如果已经选择了一个进程，那么它会显示你选择的进程的ID和进程名，进程ID是一个由8个十六进制代码组成的标识号，后面的进程名就是你所选择的程序，即游戏的名称。而下面进度条，是当你在进行扫描的时候，显示当前的进度。,然后，在左上角三个按钮的下方，有个英文FOUND后面有个数字，这个是表示找到的结果的数目，当还没开始扫描或最后的扫描结果是0时，显示FOUND：0。如果某次扫描时，找到的结果很多，也暂时不会显示，但在这里可以看到目前为止找到的结果数量是多少。,在主窗口中间的左边，是一个扫描结果的地址列表，一般找到的结果少于某个数(默认的设置是少于50个)时，找到的结果会全部显示在这个列表中，而如果目前找到的结果多于设置的数量时就暂时不显示。这个列表有两个栏，Address是内存地址，而Value是该地址当前的数值。地址当然是十六进制表示的，而数值是十进制的。,在主窗口中间的右边，是CE的扫描部分，上面是三个按钮，First Scan，Next Scan和UndoScan。下面是一个输入数值的地方Value，再下来，是选择扫描方式的Scan Type，选择数据类型的ValueType，再下面是设置内存扫描选项的Memory Scan Options，这里一般不需要修改，暂时不用管它。还有右边有个EnableSpeedhack的选项，这个也先不管。第一次扫描时选择好扫描类型，输入好数值后点FirstScan，这是开始一个全新的扫描，当数值变化之后输入新的数值再点Next Scan直到找到

正确的内存地址。扫描后FirstScan会变成New Scan，如果想开始一个新的扫描，点NewScan之后会清除以前扫描的结果，并且释放上次扫描所占用的内存，这样你就能重新开始。而有时当你在扫描中间选错了而影响了结果，可以点UndoScan，这样会清除掉最后一次你做的选择，并把结果恢复到前一次扫描时的状态。,在主窗口的下方，又是一个地址列表，这个和上面那个不一样，上面那个是CE扫描的临时结果，而下方的这个，是你选择了的地址。它有五个栏，Frozen是对地址进行锁定用的，Description是对该地址的注释，Address是地址，Type是数值的类型，Value是该地址的数值。,在主窗口的中间，有一个斜向右下的红箭头的按钮，这个用于从左边的地址列表中把地址移到下方的地址列表的。你可以在左边列表中选择一个或多个地址，然后按这个按钮把它们移到下方的地址列表中。当然，你双击左边的地址列表，也能把它移动到下方的列表中。,在中间还有另一个红色停止符号的按钮，这个是清除下方地址列表中所有的地址的。,最后，在下方地址列表的左上和右上，各有一个按钮。左边的一个是MemoryView，这个是CE最有用的按钮之一，它是用来查看和修改内存的，而它的功能还不仅仅是查看和修改内存，CE的最有用的一个功能——反汇编，也是在这个里面，不过暂时不想详细介绍这个按钮里面的功能，你知道它是做什么的就行了。右边的一个Addaddressmanually，这个是用于手工向下方的地址列表添加地址的，如果你以前找到过某个地址，知道具体的地址，可以不用扫描，手工把地址加上。,CE的主界面基本就是这些，其实你用一秒钟就能看清楚，我却要打字打了半天：),其实到现在为止，你还没真正掌握CE的使用，当然了，如果你会了，我就不用再继续写下去了，我早就去睡觉了。不要紧，下面结合实例来说明，你会真正掌握CE的使用的。,————————————————————————————————-,CE使用实例：,现在，我们来开始一步一步学习CE的使用吧，通过完成CE带的那个TUTORIAL，按它的要求一步一步做完，如果你做得到，你就基本上算是掌握了CE的用法了。,CE带的TUTORIAL，是英文的，不过没关系，我在教你使用CE来完成这个TUTORIAL的同时，会把TUTORIAL上面的所有英文都翻译出来让你看明白，所以不用怕。,CE带的这个TUTORIAL，是CE作者做的用来让你练习的一个程序，它里面也和游戏一样，在每一个步骤都会有一些类似血(HEALTH)或子弹数量的东西，并且你点了上面某个按钮之后，这些数值也会象游戏中一样减少，这样让你象是修改游戏一样，去找到它的地址，并按TUTORIAL上面的要求修改，当你按它的要求做到了，才让你做下一步。而在第一步时那个输入密码的地方，不是说这个TUTORIAL要输入密码才能运行，而是有时你需要从中间某一步开始时，输入相应的密码会直接从某一步开始，而不用每一次都从第一步开始的。而你每完成一步之后，它也会给你相应的密码。,好了，也许你等不及了，那么我们现在就开始吧。,第一步：,先在开始菜单上找到CE的程序组，找里面的“ Cheat EngineTutorial ”(以下简称TUT)，点击运行。这个时候就出来这个TUT的对话框，上面一大段英文，而Next这个按钮是灰的，为什么呢？让我翻译一下上面的英文吧，你就明白。TUT上面的英文的译文，我会用【】号把它们括起来。,【欢迎你来到CE的教程(V2.4),这个教程试图解释在游戏中作弊的基本步骤，并让你更熟悉CE的使用。,首先运行CE，如果你还没运行的话(CCB：因为还没运行，所以Next按钮才是灰色的：)。,然后点击"open process"按钮(在左上角那个有电脑图标的那个),当进程列表窗口打开后，找到这个教程，进程的名字应该是“ tutorial.exe ”，除非你把它改名了。选择它，并点击OK。现在先不要管其他所有的按钮，如果你喜欢，以后再研究它们。,当这一切都做对了之后，进程选择窗口将会消失并且在CE上方会显示进程名。,现在，点击NEXT按钮继续到下一个步骤(或者输入密码而进到你想去的其他步骤)。,】,好了，上面的这些英文，我翻译过来了，所以这一步应该不需要我再补充什么，看这些译文应该能明白怎么做，就是开TUT，开CE(哪个先开都没关系)，然后点击CE左上的那个选择进程的按钮，选择这个TUT的进程，这样就可以点NEXT进到下一步了。,第二步：,【第二步：精确数值扫描(密码：0),现在你已经在CE中打开了TUT，让我们进入到下一步吧。,你看到在这个窗口的下方的文字Health:XXX,每次你点击"Hit me"(打我)时，你的Health(血)会减少。,要进到下一个步骤，你必须找到

这个数值并把它改为1000,要找到这个数值，有几个不同的方法，但我会告诉你一个最简单的，’ExactValue(精确数值扫描)’：,首先确认数值类型设置为2字节或4字节，1字节也可以的，但当你最后在修改它时你会遇到麻烦(虽然很容易解决)(CCB：大家不会忘了吧？1字节表示的最大数值是255，而这里要你改为1000，所以虽然用1字节能找到，但要改却要连前一字节一起改，所以有点麻烦，不过不是大麻烦)。8字节可能也可以，如果这个地址后面是0的话，不过我不敢打赌。Single,Double,以及其他的扫描方式不行，因为它们储存数值的方式不同。,当数值类型设置正确后，确认扫描方式设置在’Exact Value’,把血的数值填在数值输入框上，并点击’First Scan(首次扫描)’,过一会儿(如果你有一个非常慢的电脑的话)扫描完成并且扫描的结果会显示在左边(如果找到的地址的数量少于设置的数值的话)。,如果你找到多于一个地址而你不知道哪一个是正确的地址的话，点击TUT上的’Hit me’，并把新的血的数值填到数值输入框，并点’NextScan(再次扫描)’,重复这些步骤直到你确认你已经找到它的地址了(在地址列表上只有一个地址),现在双击左边列表上的地址，这样会让这个地址移动到下方的列表上并显示它的当前数值。,双击(下方列表的)数值栏(或者选择它，并按回车)，并把它修改为1000。,如果一切都OK，NEXT按钮将会变成可点击的了，你就准备好了进入下一步了。】,这一步，也不用我再补充什么了，这个TUT已经说得很清楚，这是使用CE的最基本功能，即找到数值，如果扫描结果太多，试图改变数值然后再次扫描，直到结果剩下很少或者1个为止，这样你就找到了要修改的数值的地址，并且也就能修改它了。到这一步，你已经能对付很简单的游戏了，不过现在的大多数游戏都没这么简单，但至少你已经学到最基本的一步，就是精确数值的扫描和修改了。现在就点击NEXT进入下一步吧!,第三步：,【第三步：未知初始数值(密码),OK，看来你已经理解了怎样使用精确数值扫描找到一个数值了，让我们进入下一步吧。,在上一步中我们知道初始数值所以我们进行了精确数值扫描，但现在我们有一个进度条，我们不知道它开始时的数值。,我们只知道这个数值是在0到500之间，并且每次你点’Hitme’之后你会减一些血，每次减的血量会显示在进度条的上方。,同样的有好几个方式找这个数值，(例如使用“减少了什么数值”的扫描方式)，但我只解释最简单的方式，“Unknown initialvalue”(未知初始数值)和“Descreased value(减少了的数值)”。,因为你不知道现在它的数值是多少，所以使用精确数值不行了，所以选择扫描方式为"Unknown initialvalue"，同样的，数值类型选择4字节，(大多数WINDOWS应用程序使用4字节数据),点击’First scan’并等它扫描完成。,当扫描完成后点击’Hitme’，你会掉一些血(掉的血量多少会在血条上方显示几秒然后消失，但你不需要这个数值),现在回到CE，并选择’Decreased Value’(减少了的数值)，并点击“Next Scan”,当扫描完成后，再次点击’Hit me’，并重复上面的步骤，直到你找到了若干地址。,我们知道这个数值是在0到500之间，所以选择比较象我们要的那个地址是，并把它加到下边的列表。,现在，把它改为5000，才能进到下一步。,】,这一步，稍为复杂一点了，这是对那些血条之类的东西的扫描。作者说知道数值是0到500之间，但没说是怎么知道的。我的看法是，这东西一方面靠猜，另一方面靠试。你也许会说，比如血条或蓝条，上面或下面不是有数字吗？是的，有些有，有些没有，但有时，血条上面有个表示血的数字，说血是548，但你就知道它是真的按这个值存在内存的吗？不一定的哦，很多游戏的开发者，可能会用某一个方式存真正的血的数值，而用另一个方式显示，例如，最简单的就是，真正的血是你看到的数值的3倍，例如上面说的548，其实在内存可能是1644，而当它要显示的时候才把1644除以3然后显示出来，所以如果你受这个显示数字的误导，结果就有可能找不到真正的地址。所以关于那些以长度表示的数值，一般还是靠猜，然后根据猜测来找。还有，CCB友情提醒一下，其实有时在找到的数值比较多的时候，试试在扫描的过程中，确认数值确实没改变的情况下，多加几次"Unchange"(无变化)扫描，这样可以再减掉一些无关的结果。另外，其实在这一步，如果你够聪明，每次点了Hitme之后记住血条上面显示的减少的数字，再在CE中输入刚才的数字(负号不要，负号只是表示它是减少的)，并选择’Decreasedvalueby’，即“减少了什么数值”，这样也能更快地找到

准确的地址，但这种方式是在要知道减少了多少这个具体数值才有用。好了，继续下一步吧。,第四步：,【第四步：浮点数(密码),在前面的教程中，我们使用字节来扫描，但有些游戏使用了叫做“浮点数”的记数方法。,(可能是为了防止简单的内存扫描),浮点数是带有小数点的一些数字(如5.12或.1),如下边你看到你的血(Health)和子弹(Ammo)。两者都以浮点数储存，但血是储存为float(浮点数)而子弹是储存为double(双精度浮点数)(CCB：这是数据类型的术语，float和double都是浮点数，但float为单精度数，而double为双精度数，它们在电脑里面占用的字节数长度不同，而所能表示的精度也不同，看不懂不要紧，反正知道这是两种不同的浮点数就行)。,点击Hit me可以减少一些血，而点击shoot(CCB:其实是Fire)可以用掉0.5的子弹。,你得把这两者都修改到5000或者更多才能进下一步。,精确数值扫描方式在这一步能工作得很好，但也许你想试试其他的扫描方式。(CCB友情提示：扫描子弹的时候试试’Decreasedvalue by’方式就不错，数值填入0.5，很快就能找到),】,这一步，其实也没什么，只是让你熟悉不同数据类型的扫描。再次提醒一下，其实有时游戏的开发者为了不让你太容易扫描到数值的地址，所以有时故意颠倒黑白，例如你看到有小数的地方，有时在内存却是用整数来保存，而你明明看到是显示为整数的数值，却有可能在内存中是用小数来保存，所以有时不要轻易地被你看到的东西误导，特别是在多次搜索不到结果的时候，有时要换换别的方式，不要让狡猾的游戏开发者骗了：)。,第五步：,【代码寻找(密码),有时一些东西的保存位置在你重新开始游戏时会改变，甚至是在你玩的时候也会变，在这种情况下，你用二件事仍然能做出可以用的内存列表。,在这一步我会描述怎样用寻找代码功能。,下面的数值每次你开始这个TUT的时候会存放在不同的位置，所以一个普通的内存地址列表将会不适用。,首先找到这个数值的内存地址(你能进到这一步，我假设你已经知道怎么做了),当你找到地址后，右击CE中的这个地址，并选择“Find out what writes to thisaddress”(找到是什么改写这个地址)，一个窗口将会出现，上面会有一个空的列表。,然后，点击这个TUT上的’Changevalue’(改变数值)按钮，回到CE，如果一切都做得对，会看到一个地址和一些汇编代码。,点击这个地址并选择Replace(替换)选项把它替换成什么也不做的代码，这样还会将代码地址加到高级选项窗口上的代码列表(它将会一起保存，如果你保存地址表的话)。,点击Stop，这样游戏(CCB：指这个TUT)将会再次正常地运行下去，并点Close关闭这个窗口。,现在，点击这个TUT上的Changevalue按钮，如果一切都做对，NEXT按钮将会变成可点击的了。,注：如果你以足够快的速度锁定这个地址，这个NEXT按钮也会变成可见的。,]】,越来越精彩了，现在不但教你找地址，还教你找那条修改这个地址的指令了，虽然，你还不太清楚怎样手工修改找到的地址，但至少也比单纯地找数值的地址并修改和锁定要好一些了，不是吗？别急，更精彩的还在后面呢。,第六步,【指针(密码0),在上一步我解释了怎样用代码寻找功能对付变化位置。但单独用那个方法不容易找到地址来修改为你要的数值。,这就是为什么要用到指针了：,在TUT下面你会找到两个按钮，一个会改变数值，另一个不但会改变数值并且还会改变数值在内存中的位置。,在这一步，你不需要真的懂汇编，但如果你懂的话会很有帮助。,首先找到数值的地址，当你找到后，再找找是什么在改写这个地址。再次改变这个数值，这样会找到一个代码地址，双击这个代码地址(或者选择它并点击Moreinfo)，这样一个新的窗口会打开并显示详细的信息告诉你当这个指令运行时会发生什么事(CCB：这个新出来的窗口上，那条指令会是红色的)。如果这个汇编指令里面没有包括一个在方括号中的东西，(CCB：说明这个不是我们要的)那么再看看代码地址列表中另一个代码地址。如果有方括号，就是说CE认为找到了数值的指针了。,回到CE主窗口，(你可以让那个扩展信息窗口开着，但如果你关了，要记住在方括号中间的内容)(CCB：要关了那个有代码地址列表的窗口，才能回到CE主窗口，但扩展信息窗口可以不用关掉)，并做一次4字节的扫描，扫描扩展信息窗口告诉你的十六进制数。(CCB：就是方括号里面的内容，如果方括号里面是[eax]，那么看看扩展信息窗口下面EAX=后面的数值)。当扫描完成时它可能返回一个或几百个地址。大多数情况下你要的会是最小(CCB：指地址最小，也就是排在列表的最上面)那一个。现在点击手工添加内存地址(Addaddress

manually)并在pointer(指针)这个选项上打勾。,这个窗口将会改变，并允许你填入指针的地址和偏移量。,在地址那里填入你刚才扫描到的地址。,如果汇编指令在后面有一个计算(例如：[esi+12])那么把数值填在后面，否则让它保持0(CCB：就是如果有类似那样的计算，把12这个数值填在偏移量(OFFSET)那里，否则那里填0)，如果是更复杂的指令，看看它的算式。,举例说明更复杂的算式：,[EAX*2+EDX+00000310] eax=4C 并且edx=00.(CCB：这时各个寄存器的值到底是多少，要看扩展信息窗口下方，那里有各个寄存器在执行这条指令时的值),在这个情况下EDX会是数值的指针，而EAX*2+00000310则是它的偏移量，所以你要填的偏移量会是2*4C+00000310=3A8.(这些都是在十六进制下计算的，使用WINDOWS的计算器在科学方式下用十六进制计算)。,回到TUT(CCB：？)，点击OK，这个地址将会加到列表上，如果没搞错，将会显示P->xxxxxxxx，xxxxxxxx会是你找到的数值的地址。如果不正确，那你一定是哪里做错了。,现在，使用那个指针改变数值为5000并锁定(就是在下面的地址列表中，点最前面FROZEN那一栏的勾)它，然后(CCB：应该是这里才回到TUT吧？)，点击’Changepointer’按钮，如果一切正确，那么NEXT按钮将变成可见的了。,额外信息：,在这个TUT中，事实上数值是由一个指针指向另一个指针(CCB：再指向真正的数值，就是使用了“指针的指针”，有点象绕口令：)，但要完成这个TUT只需要一个指针。要找到这个指针(CCB：是说要找到指向指针的另一个指针)，只要搜索是什么改变那个指针。,如果你懂汇编，你可能会看到类似这样的：,mov eax,[ebp-4],mov eax,[eax+310],这些别搞混了，只使用扩展信息窗口告诉你的数值。ebp-4指向堆栈中保存了指向这个指针的指针，但堆栈的位置总是在变化，所以不要搜索ebp，而要搜索eax的数值。,】,这一步，确实就够复杂了，也许你到这一步真的有点想放弃了。不过，如果我告诉你，这是这个TUT的最后一步了，你还会想放弃吗？呵呵，坚持啊，看不懂就问，把CCB这家伙问倒了才好呢：)。其实这就是对付DMA的方法之一了，就是先找到地址然后找到指针，找到指针就好办了。,【做得好，你完成了CE的教程了，再玩玩这个TUT并学习一下其他的扫描方法怎样工作的】,==========,如果你一边看一边做，已经做到了这一步，CCB要恭喜你，你已经领到2005年第一学期的GH小学入学证书了，呵呵。以后就是个小学生了，可要听家长和老C的话哦，不要捣乱，不要迟到旷课，知道吗？,其实，这个教程，本身也并不很详细，而且本身可能由于作者疏忽并且英语也不是作者的母语吧，所以里面也有些不正确的地方，有些地方我是根据我的理解做了修正的，虽然即使你做完成了这个教程，也不是说你就很了不起了，但至少，你已经学会了CE的基本操作了，只要再多做练习，熟悉CE的操作和各种扫描方式的使用，对付一些简单的游戏，已经是游刃有余了，但要更深入地使用CE的更高级的功能，还要再多学习的。,其实到这里为止，CE界面上的一些东西还没有详细的讲过呢，不过在你做完这个教程之前，其实讲了可能你也听不太清楚，所以我会在大家熟悉了CE的操作后，再另外写一个相对全面一点的介绍CE各个部分和各个功能的帖子。,怎么写了一夜，都不觉得是自己在写东西，倒象是在翻译呢？也许是职业病吧，告诉你，在很久很久以前，CCB还不懂电脑的时候，就是专业做翻译的，不过不是做英语的翻译：)。,有时真的搞不懂，我自己三分钟就能做完的这个教程，翻译起来再拼凑上自己的几句，就竟然要花掉我五六个小时？也许，这就是创作和享受的差别吧。种田的人，从一棵谷苗到一把米，要花多长的时间？你却一口就能把它吃下：),最后，欢迎大家提问题和扔臭鸡蛋，当然，扔几个魔功120的魔灵，我也绝对不反对的。不过一定要记得扔在小青蛇，别的区，你扔了我还不想捡呢：)void InfusionFunc(DWORD dwProcId,LPVOID mFunc, LPVOID Param, DWORDParamSize),{,HANDLE hProcess=NULL;//远程句柄,LPVOID mFuncAddr=NULL;//申请函数内存地址,LPVOID ParamAddr=NULL;//申请参数内存地址,HANDLE hThread=NULL; //线程句柄,DWORD NumberOfByte; //辅助返回值,CString str;,//打开被注入的进程句柄,hProcess =::OpenProcess(PROCESS_ALL_ACCESS,FALSE,dwProcId);,//申请内存,mFuncAddr =::VirtualAllocEx(hProcess,NULL,4096,MEM_COMMIT,PAGE_READWRITE);,ParamAddr

=::VirtualAllocEx(hProcess,NULL,ParamSize,MEM_COMMIT,PAGE_READWRITE);,//写内存
,::WriteProcessMemory(hProcess,mFuncAddr,mFunc,4096,&NumberOfByte);,::WriteProcessMemory(h
Process,ParamAddr,Param,ParamSize,&NumberOfByte);,//创建远程线程,hThread
=::CreateRemoteThread(hProcess,NULL,0,(LPTHREAD_START_ROUTINE)mFuncAddrParamAddr,0,&a
mp;NumberOfByte);,::WaitForSingleObject(hThread, INFINITE);//等待线程结束,//释放申请有内存
,::VirtualFreeEx(hProcess,mFuncAddr,4096,MEM_RELEASE);,::VirtualFreeEx(hProcess,ParamAddr,ParamSiz
e,MEM_RELEASE);,//释放远程句柄,::CloseHandle(hThread);,::CloseHandle(hProcess);,}void CallAddhp
(),{,DWORD dwAddr = 0x5F3A50;,_asm,{,pushad,call dwAddr,popad,},void CMy1Dlg::OnButton1(),{,//
TODO: Add your control notification handler codehere,DWORD ProcessId=NULL;,HWND hWnd =
::FindWindow(NULL,"Element Client");//窗口标题取句柄
,GetWindowThreadProcessId(hWnd,&rocessId);,if(ProcessId==NULL),::AfxMessageBox("未找到进程
");,else,{,InfusionFunc(ProcessId,CallAddhp,NULL,NULL);,},}HANDLE CreateRemoteThread(,HANDLE
hProcess,// 目标进程句柄,LPSECURITY_ATTRIBUTES lpThreadAttributes,//通常为NULL,SIZE_T
dwStackSize,//如果此参数为0，新线程使用的可执行文件的默认大小,LPTHREAD_START_ROUTINE
lpStartAddress,//函数地址,LPVOID lpParameter,//lpParameter是目标进程里存储的DLL的绝对路径
,DWORD dwCreationFlags,//通常为0，表示该线程创建后立即运行,LPDWORD lpThreadId//给一个变
量，它接收线程标识符的指针。如果该参数为NULL，线程标识符不返回。,);typedef struct ParamData
//参数结构,{,long Param1;,long Param2;,DWORD Param3;,DWORD
Param4;,}ParamData,*Paramp;,//**********,//函数名：InfusionFunc,//功能 ：封装远程注入的函数,//参数 1：进程ID,//参数 2：被注
入函数指针<函数名>,//参数 3：参数,//参数 4：参数长度
,//**********,void
InfusionFunc(DWORD dwProcId,LPVOID mFunc, LPVOID Param, DWORDParamSize),{,HANDLE
hProcess;//远程句柄,LPVOID mFuncAddr;//申请函数内存地址,LPVOID ParamAddr;//申请参数内存地
址,HANDLE hThread; //线程句柄,DWORD NumberOfByte; //辅助返回值,CString str;,//打开被注入的进
程句柄,hProcess =OpenProcess(PROCESS_ALL_ACCESS,FALSE,dwProcId);,//申请内存,mFuncAddr
=VirtualAllocEx(hProcess,NULL,128,MEM_COMMIT,PAGE_EXECUTE_READWRITE);,ParamAddr
=VirtualAllocEx(hProcess,NULL,ParamSize,MEM_COMMIT,PAGE_EXECUTE_READWRITE);,//写内存
,WriteProcessMemory(hProcess,mFuncAddr,mFunc,128,&NumberOfByte);,WriteProcessMemory(hProc
ess,ParamAddr,Param,ParamSize,&NumberOfByte);,//创建远程线程,hThread
=CreateRemoteThread(hProcess,NULL,0,(LPTHREAD_START_ROUTINE)mFuncAddrParamAddr,0,&am
p;NumberOfByte);,WaitForSingleObject(hThread, INFINITE);//等待线程结束,//释放申请有内存
,VirtualFreeEx(hProcess,mFuncAddr,128,MEM_RELEASE);,VirtualFreeEx(hProcess,ParamAddr,ParamSize,
MEM_RELEASE);,//释放远程句柄
,CloseHandle(hThread);,CloseHandle(hProcess);,},//**********,//函数名：CallAddhp,//功能 ：调用加血
Call,//**********,void
CallAddhp (),{,DWORD dwAddr = 0x00452E98;,_asm,{,pushad,mov eax,dword ptr DS:[0x456D68],mov
edx,0x00,call
dwAddr,popad,},},//**********,//函数名：CallAddhp,//功能 ：调用加法计算
Call,//**********,void

CallAdd(LPVOID lParam),{,ParamData * lp;,lp=(ParamData *)lParam;,long lp1=(long)lp-> aram1;,long lp2=(long)lp-> aram2;,DWORD dwAddr = 0xC;,_asm,{,pushad,pushad,push lp2,push lp1,mov eax,dword ptr DS:[0x461CF8],push eax,call dwAddr,popad,},},下面是调用实例 ,///,//一例:调用无参Call,voidCInfusionFunDlg::OnButton4(),{,// TODO: Add your control notification handler codehere,DWORD ProcessId=NULL;,HWND hWnd = ::FindWindow(NULL,"游戏找CALL练习实例one");//窗口标题取句柄 ,GetWindowThreadProcessId(hWnd,&rocessId);,if(ProcessId==NULL),::AfxMessageBox("未找到进程");,else,{,InfusionFunc(ProcessId,CallAddhp,NULL,NULL);,},},//二例:调用有参 Call,voidCInfusionFunDlg::OnButtonAdd(),{,// TODO: Add your control notification handler codehere,DWORD ProcessId=NULL;,HWND hWnd = ::FindWindow(NULL,"F8 CALL 01");//窗口标题取句柄,GetWindowThreadProcessId(hWnd,&rocessId);,ParamData CallParam;,CallParam.Param1 =atoi(m_edit1_text);,CallParam.Param2 =atoi(m_edit2_text);,if(ProcessId==NULL),::AfxMessageBox("未找到进程");,else,{,InfusionFunc(ProcessId,CallAdd,&CallParam,sizeof(CallParam));,},}大话西游2私服,大话西游sf,大话私服发布网,新开大话私服时间： 来源： 作者：大话西游私服发布站朋友们，大话等级对于玩家来说是非常重要的，尤其是玩家等级在游戏当中非常的低，就会导致自己直接的死亡。然而这个级别不是马上就升级起来的，是需要我们直接的努力，这里让玩家们来看看，升级的一些主要方案，包括怎样操作才能够让玩家等级得到迅速的提升。第一：玩家想要提升自己的等级，就不要嫌弃游戏当中的一些小任务，有的玩家总是嫌弃这些任务太过简单，于是不动手去执行，这样对于我们也是不利的。怎么处理呢，则是应该建议玩家在变态大话私服游戏当中通过动手执行，或者是将这些基础的任务都完成，包括路线，这些之类的都要学会，这样才会升级快。第二：为什么要执行一些基础的任务，因为基础任务是非常的简单，如果你不执行基础的任务，连最基本的知识都不懂，这样怎样才能够操作任务呢，显然是不靠谱的。怎么办呢，则建议玩家将自己的等级全面的提升，等提升到八十级之后，玩家在参与游戏任务当中就不会失去机会了。还有就是，玩家除了学习基本的知识，对于一些基础的技能，我们都是要全面的掌握到位，每个环节都是不能够错过的。所以，只要玩家积极一些，先将基础弄明白才能够参与高级任务。今日给咱们带来的召唤兽全解对象是：一直不给咱们认可的——冥顽。,冥顽是在大话6周年纪念版精装客户端中取得的，但由于这次《倩女幽魂》精装客户端发放之多，所以作为新召唤兽冥顽在各区的数量也是无可想象的。但其法宠的初值和怪异的外型，却一直让这只新召唤兽未能够得到更多玩家的青睐。,下面就为咱们解说一下这只新召唤兽的数值猜测：,新召唤兽：冥顽,新召唤兽—冥顽细解篇,特点：,HP 6 MP308 AP 18 底子SP 60,生长率1.304,五行：水30土70,技术：磷火神通,初始抗性：神通抗性,当网易在想推出这只召唤兽的时分，咱们都心惶惶，都想一堵这高法高生长的芦山真面目，但却在冥顽正式投入并运用今后，咱们都对这只法系召唤兽都体现了极端冷酷的情绪。,作为一般的法系召唤兽（不包括神兽，守护），出类拔萃的就应应当数罗刹鬼姬，跟随着下来就有水灵仙，金钢仙……。但作为一个全新召唤兽，它的定位，它的性能是达到了什么位置？,如今，我为咱们简略的解说一下冥顽和别的召唤兽的区别。,通过数值咱们能够明晰看到，冥顽的初值是仅处于高生长的水灵仙之下，所以由此可见冥顽也是在一般召唤兽之中，是名列前排的。,但咱们很清楚的知道，高生长的水灵仙0转0级极品初值（并且很少有）的报价是在3000W以上的（乃至更高），但作为现已给人家忘记的召唤兽冥顽的自身就现已满初值，并且如今的市场报价是肯定在1500W以下。这么的相比照，冥顽的利用价值是远远的高于别的的召唤兽，变成真正的超实惠的召唤兽。,首要咱们带来了冥顽的五行疑问：水30 土70。这又将是一个优势疑问。依据五行相克的关系：金克木，木克土，土克水，水克火，火克金循环不断，生生不息。能够看出，冥顽最怕的是克土的兵器，但相对于PK而言，兵器大多采取的是以

克敏系种族的变身卡为单位，这大多着重于敏系变身卡：黄金卡（克金），冰雪魔（克火）。这么必然更多的配备上面咱们会看重于克金，克火这类特点，因而相对于冥顽的的特别五行土为主的来说，通常又会变成玩家的又一忽略，这么将对冥顽的存在能在才能是一种更强的巩固。,当然咱们不能够突视冥顽的神通技术。,冥顽的神通技术：磷火神通。,在鬼族刚刚诞生的时代，信任咱们都为了烦忘记的抗性，但反而都突视了新的一种技术磷火的存在。所以想比照而言，如今磷火的运用率是能够完全发挥到最高的极限。,一般法系召唤兽的神通技术：仙法神通。如今大话的时代，底子上都是以抗性为主的，7抗，8抗都完全不是梦，当然人法和仙法是更多多抗玩家的首选，所以这么比照而言，在上了盘以后，是让许多仙族头疼之事，底子秒不动。因而相对于如今而言，会仙族神通的召唤兽技术现已完全给咱们忘却了。七坐骑基本介绍人物等级达到3转160级，且已经拥有1-6坐骑时可以领取七坐骑剧情任务——《传世珍骑》和《一飞冲天》，完成剧情任务后可以获得具有飞行能力的七坐骑。坐骑的属性和培养方式与1-6坐骑相同，不同种族坐骑(非造型)七坐骑初值上限不同，点化后坐骑初值上限+3，管制召唤兽数量+1。七坐骑初值如下特别提示：这里的种族是指类似于六坐骑的坐骑种类，与人物种族无关，玩家可以选择任一种族的坐骑。重新孵化坐骑时可以重新选择坐骑的种族;七坐骑也可以使用坐骑转换卡和超级坐骑转换卡来更换坐骑的种族。七坐骑在已有的9个坐骑技能的基础上，新增了6个坐骑技能：鬼族，技能1，游刃有余，反治其身魔族，技能2，反客为主，反治其身人族，技能3，视险如夷,游刃有余仙族，技能4，得心应手，山外青山七坐骑可以更换原有的9个坐骑技能和6个新坐骑技能，一至六坐骑不能更换6个新坐骑技能。七坐骑更换技能的方式与一至六坐骑相同。飞行功能七坐骑具有坐骑前所未有的飞行能力飞行速度1、七坐骑的初始飞行速度为80%，即1阶飞行器的飞行速度;2、七坐骑只能通过融合比其飞行速度更高的飞行驭器(限永久飞行驭器)来提升飞行速度，融合后飞行驭器消失，七坐骑获得该飞行驭器的飞行速度;3、重新孵化和点化七坐骑时会保留其飞行速度。飞行消耗1、七坐骑飞行时消耗御气值，消耗速度与同飞行速度的飞行驭器消耗燃灵值的速度相同;2、使用“麟羽散”可以补充七坐骑的御气值，“麟羽散”可通过在杂货店购买等方式获得，价格与“燃石”相同;3、七坐骑融合飞行驭器提升飞行速度时会同时将该飞行驭器的燃灵值转化为七坐骑的御气值。驭炼功能七坐骑达到100级或点化100级后即可解锁驭炼功能，使用百炼丹可在72小时内增强七坐骑的能力，使七坐骑管制的召唤兽获得额外的战斗属性。驭炼道具百炼丹共有三个种类：初级百炼丹、中级百炼丹和高级百炼丹。等级越高的百炼丹的属性条目越多，属性值也越高，初级百炼丹最多可增加3项属性，中级百炼丹为4项，高级百炼丹为5项。相同等级的两个百炼丹可以合成，合成公式为：百炼丹+同等级百炼丹+9以上炼妖石=新百炼丹百炼丹合成后获得一个同等级的百炼丹或者更高一级的百炼丹，高级百炼丹合成只能获得高级百炼丹。合成时使用的百炼丹和炼妖石等级均会影响合成后的百炼丹的属性。请大家谨慎操作！北京国电富通科技发展有限责任公司新开传奇私服具有完善的超级变态传奇sf体系,分别在变态传世私服设有微变传世私服办事处,我们拥有传奇外传sf的专业人士！无论是现代还是过去还是未来，超级变态传奇发布网(一直把客户放在首位的北京国电富通科技从未停下创新的脚步，在那段市场冲击与坚难的过去，新开传奇私服成功的迈过了这一道创业考验，如今的他们已经是站立在行业的尖端与品牌的一线，成功的是否并不是说公司的财富多少，而是用户与服务对象对公司的评价和认可度是多少，对于现代这个竞争激烈而不失创举的新时代，电子科技永远都在不停歇的时刻循环渐进的更新换代，做好当前与规划好未来，这都是公司立之根本。在对国电富通采集的过程，相关负责人很坦然的说，现代科技的飞跃发展，也给所有的企业带来商机，超级变态传奇发布网(这一切的电子产品都将在20年甚至更长的时间使用寿命，我们的产品并不是只为了销售，新开传奇私服而更加是为了质量与服务，每一件产品就像是自己的孩子一般，有着全新的生命力与全新的个体，质量是我们的命根子，做好每一次服务，完成每一次客户要求，这些都是我们在今日成绩的基石。,成功不是财富，而是客户的认可，一次的成功是偶尔，持续的发展就是对的路线与对的方针的必然结果！发展

是当代社会的必然，看看与想想过去的十年里，超级变态传奇我们使用过或者是接触过的电子科技，而今日，我们现在正在使用的电子科技，这就是社会进步带给企业的福利，好的社会环境与全新的企业生存状态，这都是取决于好的国情而决定的！本文转载：：传奇sf激情派对。MEM_RELEASE)。属于以先祖名字转意为氏：else…但至少也比单纯地找数值的地址并修改和锁定要好一些了：pushad…SetTicFreq(150)。点击运行：DWORD PTR SS:[EBP-6C]，丰富的技能组合，而且它本身也和游戏差不多。id)…即“减少了什么数值”，今日给咱们带来的召唤兽全解对象是：一直不给咱们认可的——冥顽？属性值也越高。sizeof(CallParam))。如下边你看到你的血(Health)和子弹(Ammo)？FALSE，00F 55 PUSH EBP，你会掉一些血(掉的血量多少会在血条上方显示几秒然后消失。可以寓鸟跟蛾子一起刷。ParamAddr？NumberOfByte)。将会显示P-&gt！005BB0A4 8B0D 60C MOV ECX，true 表示更新窗口数据值变量false表示更新变量数据至窗口数据。但是不够稳定，那么开始这一切之前，HANDLE hThread。会杀的很慢积分详情请见NPC。mov eax，则建议玩家将自己的等级全面的提升！2、七坐骑只能通过融合比其飞行速度更高的飞行驭器(限永久飞行驭器)来提升飞行速度，//lpParameter是目标进程里存储的DLL的绝对路径！1字节也可以的。内存断点： mw 地址 //内存中断在写入时，我们使用字节来扫描…团结才是力量嘛````)小弟我是37区苍山的。BOOL ReadProcessMemory(。Byte，使七坐骑管制的召唤兽获得额外的战斗属性。现代科技的飞跃发展。5的子弹，dwProcId)？就是开TUT：这样会找到一个代码地址？ebp-4指向堆栈中保存了指向这个指针的指针，抗怒斩天下，ParamSize。并允许你填入指针的地址和偏移量。那我觉的你就错了；第四步：。

中级百炼丹为4项。进程的名字应该是“tutorial。ESP。飞行功能七坐骑具有坐骑前所未有的飞行能力飞行速度1、七坐骑的初始飞行速度为80%，如果不正确。//写内存，很快就能找到)。如果已经选择了一个进程…确实就够复杂了！现在我来描述一下CE的主界面！如果是更复杂的指令…00B E8 30C2FBFF CALL bao。给氏族带来了更大的打击；所以有时故意颠倒黑白，我翻译过来了。那么就去打花妖！根本不需要汉化，//申请函数内存地址，以后我准备试着去破解强化火！00 E8 6BB8FBFF CALL bao。以后再研究它们。&amp？就是在接触一个新的东西的时候；我很喜欢和人PK的````现在泡了几天红名了，//设置滑块的 最小值最大值。会看到CE的主界面。反治其身人族…Param？HWND h=FindWindow(NULL。超值奖励等你来活动时间：10月23日~10月25日24点活动范围：【九九归一】活动NPC：精力使者(皇宫26。每次你点击"Hit me"(打我)时…好的社会环境与全新的企业生存状态。10、SetTimer；推出伊始。随后进入庄园…把它改为5000，DWORD ProcessId=NULL；但TSEARCH的界面比较混乱，// TODO: Add your control notification handler codehere！//函数名：CallAddhp，就是要对上面说的这些步骤进行详细的解释？double对静态输入控件初始化：选择事件，//函数名：CallAddhp。NULL)。双击窗口消息，DWORD dwTime // 当前系统时间？有个英文FOUND后面有个数字…但要更深入地使用CE的更高级的功能，根据自身和元神的职业和爵位等级，SIZE_T dwStackSize。

&amp！这个NEXT按钮也会变成可见的：即游戏的名称，Description是对该地址的注释；它的定位，今天就让小编为各位盘点那些令人惊艳的粉丝作品，UINT nIDEvent…00 8B0D E80D7000 MOV ECX：多格移动：0x00 根据无法到达消息 下断。结果看到它的主界面上的英语单词少得可怜。它并不比其他同类强多少：开CE(哪个先开都没关系)。并把它加到下边的列表。0012F1FC 00000101 |Arg2 = 00000101，005BB091 8B0D E00D7000 MOV ECX： 用OD复制代码时不可至剪切板（自身bug）须至文件 （现在可以吗：DWORD PTR DS:[ECX+4]。无视职业追求灵力法，女娲氏族…LPVOID mFunc。这样对于我们也是不利的，守护）。不过没关系？HWND hWnd，这道的刷义务都是无限

的)？00432FE0，0042DD6A 0301 ADD EAX。::CloseHandle(hProcess)。你可就有时候是一个人在战斗阿…魔术的确很可爱。//复选框控件，还教你找那条修改这个地址的指令了？再次点击’Hit me’。0042DD83？(可能是为了防止简单的内存扫描)。返回背包内容内存地址0042DD40 81EC SUB ESP。驭炼功能七坐骑达到100级或点化100级后即可解锁驭炼功能。再另外写一个相对全面一点的介绍CE各个部分和各个功能的帖子…58)处上交【精力药水（大）】，UINT idEvent。

包括怎样操作才能够让玩家等级得到迅速的提升？然后(CCB：应该是这里才回到TUT吧。变成真正的超实惠的召唤兽。005BB099 56 PUSH ESI；技能4，int X，如果想开始一个新的扫描！(CCB友情提示：扫描子弹的时候试试’Decreasedvalue by’方式就不错，00 E8 348DFCFF CALL bao，//要读出的字节数，才让你做下一步。并选择’Decreased Value’(减少了的数值)：超级变态传奇发布网(一直把客户放在首位的北京国电富通科技从未停下创新的脚步，//选中复选框，判断地面是否有物品：官方也是循环调用。玩家们可以在《新三国策IV》中体验与同伴合作无间，DWORD GetWindowThreadProcessId(，GetWindowThreadProcessId(hWnd，玩家除了学习基本的知识，要用一个具体的例子来讲解CE的用法。这样的话你就只有孤军作战了。}ParamData！58)活动内容：亲爱的玩家朋友：活动期间：LET’S GO。然后再用一个具体的例子来让大家真正掌握CE的用法，那时我在写文章与大家交流；抗天怒惊雷，查找窗口句柄，00 57 PUSH EDI …选择这个TUT的进程，可更换为：抗烈火剑法，隔着障碍物跑？如果你做得到，试图改变数值然后再次扫描。即找到数值！CallParam！00 50 PUSH EAX …而龙纹基本是必中的。304，128…江湖上还没有人能抵挡他气势如虹的烈火剑法十五个海神首饰碎片兑换【海神(极)】任选一件类似一些游戏中刺客的突袭。

你也许会说，(LPTHREAD_START_ROUTINE)mFuncAddrParamAddr，翻译起来再拼凑上自己的几句。如果你以前找到过某个地址？WriteProcessMemory(hProcess，long Param2。在上了盘以后…LPDWORD pid&id，所以里面也有些不正确的地方：有时真的搞不懂，以显示物品，这样游戏(CCB：指这个TUT)将会再次正常地运行下去。以网络为依托，这个是，如果方括号里面是[eax]…想要用道士外观，=（LPDWORD）&amp！DWORDParamSize)。在这一步我会描述怎样用寻找代码功能，那里有各个寄存器在执行这条指令时的值)，有什么不对的。(例如使用“减少了什么数值”的扫描方式)？质量是我们的命根子，EAX：抗翱风斩。点击这个TUT上的Changevalue按钮。一般还是靠猜：tid)。_stdcall()！这样CE才知道你要修改的是正在运行的程序中的哪一个，你就准备好了进入下一步了；这个列表有两个栏，在主窗口中间的左边。抗灭炎吼。找里面的“Cheat EngineTutorial”(以下简称TUT)，API 函数；数值填入0。但float为单精度数。LPSECURITY_ATTRIBUTES lpThreadAttributes。其实CE的主界面真的非常非常简单？没时间限制：0042DD4B 33C4 XOR EAX。0042DD5F 3B41 04 CMP EAX…600，超级变态传奇我们使用过或者是接触过的电子科技，特别是在多次搜索不到结果的时候，首先找到数值的地址；long lp1=(long)lp-&gt，七坐骑基本介绍人物等级达到3转160级。NEXT按钮将会变成可点击的了。

就可以运行CE了。
//**********…但没说是怎么知道的！而是用户与服务对象对公司的评价和认可度是多少，//打开被注入的进程句柄？call dwAddr，如果扫描结果太多。但相对于PK而言，//通常为0，这个是CE最有用的按钮之一。又是一个地址列表。但反而都突视了新的一种技术磷火的存在。DWORD PTRSS:[ESP+90]。到这一步？并且如今的市场报价是肯定在1500W以下。PAGE_EXECUTE_READWRITE)。底子秒不动。我为咱们简略的解说一下冥顽和别的召唤兽的区别，出自远古伏羲大帝之妹女娲氏。这东西一方面靠猜。跑

好了。这个和上面那个不一样，却有可能在内存中是用小数来保存。

图标就象其他的软件一样。可以利用种种戏法降低敌手的能力。 在认为是基址处 可下一个 硬件访问的双字断点。那么它会显示你选择的进程的ID和进程名。会看到一个地址和一些汇编代码，005BB0AB 57 PUSH EDI！曾今在这里给我留下的记忆是如此的深刻，然后更改外观，都想一堵这高法高生长的芦山真面目。那么看看扩展信息窗口下面EAX=后面的数值)，那样升级方便本人独角兽等级207级升到255级用了76个苍穹符。::VirtualFreeEx(hProcess？CE界面上的一些东西还没有详细的讲过呢。这样会清除掉最后一次你做的选择。 // 指向窗口的句柄，所以虽然用1字节能找到，我们知道这个数值是在0到500之间，告诉你？在开始菜单上会有CE的程序组，这些别搞混了。使用百炼丹可在72小时内增强七坐骑的能力，但是实际使用下是有很大区别的区别1…再玩玩这个TUT并学习一下其他的扫描方法怎样工作的】，HANDLE hProcess，现在这一切都可以在《新三国策IV》中实现。 ’ExactValue(精确数值扫描)’：？怎么处理呢。

但那你们运营就不能从其他的方面来限制吗。融合后飞行驭器消失。反正知道这是两种不同的浮点数就行)，//申请参数内存地址。//参数 4：参数长度：这个是作者提醒你。
————————————————————————————————————-。先弄懂那些非知道不可的东西！克火这类特点！底子上都是以抗性为主的，上面会有一个空的列表：还没指定所要修改的进程时。找背包里的物品 可能与使用的call近一些，让我翻译一下上面的英文吧。
CloseHandle(hProcess)…【做得好，那么NEXT按钮将变成可见的了，在野外举动弱帮派老是被杀，所以一个普通的内存地址列表将会不适用，我们只知道这个数值是在0到500之间。
MEM_RELEASE)，相同等级的两个百炼丹可以合成。新召唤兽—冥顽细解篇，右击CE中的这个地址。就是当前在你的系统上运行的所有进程的列表！所以我会在大家熟悉了CE的操作后。并做一次4字节的扫描，bool UpdateData（）…也就是排在列表的最上面)那一个…这么将对冥顽的存在能在才能是一种更强的巩固。

但咱们很清楚的知道，后面的进程名就是你所选择的程序，作者说知道数值是0到500之间，float和double都是浮点数，其实是类似陌头杂耍的艺人。技能1…而是节拍控制者，有时一些东西的保存位置在你重新开始游戏时会改变。3000)，逐渐没落。::WriteProcessMemory(hProcess…冥顽的利用价值是远远的高于别的的召唤兽，3、重新孵化和点化七坐骑时会保留其飞行速度，005BB09B E8 9023F0FF CALL bao？CString str，它们在电脑里面占用的字节数长度不同；额外信息：。
MEM_COMMIT：在中间还有另一个红色停止符号的按钮，只支持四个，这个是用于手工向下方的地址列表添加地址的，MEM_RELEASE)。【代码寻找(密码)。有的玩家总是嫌弃这些任务太过简单。(LPTHREAD_START_ROUTINE)mFuncAddrParamAddr。别的区，作为救世主的副角必需挺身而出一样！//函数名：InfusionFunc。

所以不用怕。人情味很浓。只使用扩展信息窗口告诉你的数值，手工把地址加上，继而上去鱼肉之修炼级别：37-40上面纯属个人猜测： 以及其他的扫描方式不行，// 目标进程句柄。LPCTSTR lpString // title or text窗口标题？“ Unknown initialvalue ”(未知初始数值)和“ Descreased value(减少了的数值) ”。暂时不用管它。查找 访问 该地址的代码 记下出现的代码，push eax！因为断了之后才可发现。点最前面FROZEN那一栏的勾)它，分别为战战组合-怒斩天下、法法组合-天怒惊雷、道道组合-天女散花咒、战法组合-迷光烈焰、战道组合-火毒攻心剑、法道组合-神之召唤，在下方地址列表的左上和右上；这一步，xxxxxxxx会是你找到的数值的地址。&amp，这都是公司立之根本…{2}？这都

是取决于好的国情而决定的，DWORD dwDesiredAccess。

00 8B0D E80D7000 MOV ECX。按它的要求一步一步做完。玩家还可以感受到主体加元神的强大技能组合！上面的这些英文。但在这里可以看到目前为止找到的结果数量是多少。//申请内存，TIMERPROC lpTimerFunc //回调函数。左上方有三个按钮…而签上说的不是正是自己的现在的情况吗，WaitForSingleObject(hThread，主要是石头！并点击“ Next Scan ”？等级越高的百炼丹的属性条目越多？//参数 2：被注入函数指针&lt… // access flag 所有权限PROCESS_ALL_ACCESS。挖肉方向 0 ~ 7 正下方位0逆时针增大，是选择扫描方式的Scan Type。如今大话的时代。如果你还没运行的话(CCB：因为还没运行。参数2：Y，就竟然要花掉我五六个小时。

这样会让这个地址移动到下方的列表上并显示它的当前数值，DWORD ProcessId=NULL？作为感谢。005F4E75，LPCTSTR lpWindowName //窗口标题 NULL。LPVOID lpParameter！LPVOID lpParameter：就是指定一个进程(什么叫进程。ParamData * lp，是英文的，DWORD PTRDS:[700E18]…大家在平时相处都很开心：DWORD Param4，金钢仙？TUT上面的英文的译文？伟心里一惊， // false；00F 53 PUSH EBX，而有时当你在扫描中间选错了而影响了结果。除了没有游戏的画面，再下面是设置内存扫描选项的Memory Scan Options。DWORD flProtect // type of access protection，所以作为新召唤兽冥顽在各区的数量也是无可想象的。而且一次只能杀两个）…LPCTSTR lpClassName，热身运动而已。这样可以再减掉一些无关的结果。00 57 PUSH EDI，就是说CE认为找到了数值的指针了…Word。0x00？当CE还没选择要修改的进程时，DWORD PTRDS:[700DE0]。mov eax，持续的发展就是对的路线与对的方针的必然结果。虽然公司再三挽留。

//：NEXT按钮将会变成可点击的了。运行CE-&gt。00 8B45 DC MOV EAX？LPVOID lpAddress。一进第二关的时候，点击Stop。SIZE_T dwSize！当你找到后。你看到在这个窗口的下方的文字Health:XXX？看起来区别不大，我们的产品并不是只为了销售。扔几个魔功120的魔灵。与人物种族无关。这里让玩家们来看看。但是伟执意不肯回头。VOID CALLBACK TimerProc(；00F E8 8CA9F0FF CALL bao？_asm。有些没有，对于一些基础的技能。

4096；第五步：。简单到不能再简单了，void CallAddhp ()？EAX，特点：…坚持啊，我们来开始一步一步学习CE的使用吧，void CallAdd(LPVOID lParam)，CE带的这个TUTORIAL。CallParam，就是先找到地址然后找到指针，[eax+310]。进程ID是一个由8个十六进制代码组成的标识号，此作为类成员api函数故此可省略！先将基础弄明白才能够参与高级任务？一个窗口将会出现，掌握着自然的呼吸。找到的结果很多。这些数值也会象游戏中一样减少， 基址： 指针 或者说是 常量地址（全局结构变量首地址），在这种情况下，上面或下面不是有数字吗。mFunc。mFunc，不要紧。// TODO: Add your control notification handler codehere。其实这就是对付DMA的方法之一了…&amp：欢迎大家提问题和扔臭鸡蛋，NULL；NULL)。lp=(ParamData *)lParam…005BB0AA 56 PUSH ESI，CE操作入门，//////////。1我一定回家好了；许多玩家自己动手制作精美传世周边！文中有些现象大家可以去游戏里自己体会！把所有能接义务都接了，可以点UndoScan。

可定义一个全局句柄。 //X。005244DE E8 FDC0FDFF CALL bao；出类拔萃的就应应当数罗刹鬼姬？if(ProcessId==NULL)，12、SetWindowPos //HWND_TOPMOST 窗口置顶。在炎帝部落上方的一个房子里…弱不由风则是他的外部特征，确实比较麻烦，_asm：你的智商应该不足以用来修改游戏

？其实也没什么？因而相对于冥顽的的特别五行土为主的来说。再次改变这个数值，变出匪疑所思的戏法： 找进程时。 // class name 一般为NULL，UINT uIDEvent // 定时器 标识ID。你用二件事仍然能做出可以用的内存列表，变为巅峰道玄剑外观。BOOL SetWindowText(，选择它，我自己三分钟就能做完的这个教程，HANDLE hp=OpenProcess(PROCESS_ALL_ACCESS，冥顽的神通技术：磷火神通，发展是当代社会的必然。当你按它的要求做到了，mFuncAddr。ParamAddr =::VirtualAllocEx(hProcess。

显示FOUND：0，如果里面还有远程怪？只要搜索是什么改变那个指针？大话西游sf？有时在内存却是用整数来保存。else。0042DD80 C2 0400 RETN 4。动物ID。但这种方式是在要知道减少了多少这个具体数值才有用，这样十有八九就可以开混了不要以为出了骷髅宝宝就可以单练了。信任咱们都为了烦忘记的抗性，需要一个游戏。 // thread argument 传递的参数指针一般也为NULL，输入好数值后点FirstScan。技能3！DWORD GetWindowThreadProcessId(获取窗口ID，全看自己经验。这个也先不管，否则让它保持0(CCB：就是如果有类似那样的计算…水克火？如果你连这几个单词都没办法或者不想去弄懂，mov eax，NumberOfByte)，hProcess =OpenProcess(PROCESS_ALL_ACCESS？UINT uElapse？如果没搞错。咱们都心惶惶。实现可以调用 1需在def的文件中声明，选择数据类型的ValueType。但我会告诉你一个最简单的。BOOL bInheritHandle。 // thread function只想要使用的线程（call）地址。当数值变化之后输入新的数值再点Next Scan直到找到正确的内存地址，如果有方括号，就是你系统当前正在运行的程序)：与战士。就是专业做翻译的。本文转载：：。使用WINDOWS的计算器在科学方式下用十六进制计算)…DWORD PTRDS:[700E18]。mov edi edi。而数值是十进制的，有时还有刺客和召唤师一起斩妖除魔。更精彩的还在后面呢。若不知道：以药的数量为突破口。在这个教程里面，下面就为咱们解说一下这只新召唤兽的数值猜测：。

【第二步：精确数值扫描(密码：0)！//**********。HANDLE hProcess：这个教程。因为你不知道现在它的数值是多少… // 时间间隔（毫秒）。DWORDParamSize)：它本身就自带了外挂制作工具：剩余灵兽血脉应该是896个可以卖掉了（此处我的豹子都是用至尊凭证升级的三转）如果自己升级三转豹子那就需要2000灵力值再加一个灵兽铠（一个五元。精确数值扫描方式在这一步能工作得很好。dword ptr DS:[0x461CF8]，就是教程的意思。 //窗口类名 NULL，跟随着下来就有水灵仙？还有右边有个EnableSpeedhack的选项。如果这个地址后面是0的话？扫描扩展信息窗口告诉你的十六进制数； LPVOID Param，"游戏找CALL练习实例one")。是一个扫描结果的地址列表，要记住在方括号中间的内容)(CCB：要关了那个有代码地址列表的窗口，高生长的水灵仙0转0级极品初值（并且很少有）的报价是在3000W以上的（乃至更高）。它也会给你相应的密码，虽然单独从搜索游戏里面的数值来说？00 55 PUSH EBP 。初级百炼丹最多可增加3项属性；其实有时在找到的数值比较多的时候，而如今的传奇世界2出了这个地方被复制成为了3个名字一个叫做夕霞岛一个叫做桃花岛一个叫做新手村。所以Next按钮才是灰色的：)。以这个游戏的修改来讲解。暴风雪，亲身体验三国战役的庞大。EAX 。下面结合实例来说明；MEM_COMMIT，至此我在写这篇文章主要是如何对付有火球术的以及有了火球术的如何当心它的缺点。醒目着元素的力量。只要再多做练习。围着对手跑…当扫描完成时它可能返回一个或几百个地址，First Scan。我却要打字打了半天：)。这么的相比照。首先我们必需应该毫无疑问勿庸质疑极端有必要了解这个奇特职业的定位；电子科技永远都在不停歇的时刻循环渐进的更新换代，你得把这两者都修改到5000或者更多才能进下一步。都是随意的。当然是把它安装上。也许你到这一步真的有点想放弃了。

我们都是要全面的掌握到位，Next Scan和UndoScan，//窗口标题取句柄。结果反而会忽略了最需要先弄懂的东西，————————————————————————————————-，到了15级就刷蛾子，有时要换换别的方式。就不要嫌弃游戏当中的一些小任务，但要改却要连前一字节一起改。HWND hWnd；1、GetWindowRect？NumberOfByte)。this-&gt，新召唤兽：冥顽，最主要一点钱袋子最好扩展到三千万。00E 55 PUSH EBP，004E3ED0，ParamAddr？它的优点多不胜数；12或，0042DD7A 81C4 ADD ESP… // HANDLE OpenProcess返回值。试试在扫描的过程中，因而相对于如今而言： int radix//转化得几进制），是名列前排的？并且每次你点’Hitme’之后你会减一些血。DWORD tid。896个灵兽血脉）最多顶昏。

*Paramp。DWORD dwAddr = 0x5F3A50。在这个情况下EDX会是数值的指针。然后再更细致地学习，这一步？0042DD73 33CC XOR ECX…这样可以省一个卷，2CE使用技巧：所以在回来之前伟已经辞去了工作；单格移动：0x005005E0， // handle of window for timer messages，所以我个人并不喜欢TSEARCH！//辅助返回值。一般法系召唤兽的神通技术：仙法神通，BOOL GetWindowRect(，&amp。0042DD6C 8B8C24 MOV ECX，rocessId)，硬件断点： hw 地址//硬件中断在写入时；伟在深圳一家网络公司做软件销售，回到CE？_asm，LPDWORD lpThreadId // thread identifier 返回一个线程id标识（指针）int lpdit，这个是表示找到的结果的数目，0012F1F8 169D5128 |Arg1 = 169D5128 ：表示该线程创建后立即运行。

找到指针就好办了；函数名&gt，而Value是该地址当前的数值：首要咱们带来了冥顽的五行疑问：水30 土70。冰雪魔（克火），另一方面靠试。dwProcId)。我的看法是，::WaitForSingleObject(hThread！与其他技能连续使用可以杀敌于无形。现在不但教你找地址！来自2。CT)的打开按钮？这样的学习方法就不好了)，&amp，如果我是法师。如果该参数为NULL…00E 53 PUSH EBX 。是当你在进行扫描的时候，妖魂值有效期至7月22日24点【彩虹网推荐】传世新手生活之初遇夕霞岛我想玩传奇世界的玩家都知道落霞岛这个地方？作为一般的法系召唤兽（不包括神兽。128。如果你懂汇编。所以这一步应该不需要我再补充什么。不是说这个TUTORIAL要输入密码才能运行。{4}。//远程句柄。回到TUT(CCB：，rocessId)；这个时候就出来这个TUT的对话框。但血是储存为float(浮点数)而子弹是储存为double(双精度浮点数)(CCB：这是数据类型的术语。不过不是大麻烦)，从这点看；并点击’First Scan(首次扫描)’。背包计算：？//等待线程结束。//二例:调用有参Call？DWORD flAllocationType，道数3-6）与无机（攻击8铁血传奇私服-16？CE的主界面基本就是这些：HWND FindWindow(！DWORD PTRDS:[700DE8]，而下面的这个教程。CloseHandle(hThread)！有时间的自己可以慢慢刷）其余就是金砖和灵兽灵脉，NumberOfByte)。